Part No. 060603-10, Rev A
April 2019

OmniSwitch AOS Release 6 CLI Reference Guide

6.7.2.R06

Alcatel·Lucent Enterprise

www.al-enterprise.com

This user guide documents release 6.7.2.R06 of the OmniSwitch 6350/6450 Series.
The functionality described in this guide is subject to change without notice.

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE.

26801 West Agoura Road
Calabasas, CA 91301

Service & Support Contact Information

North America: 800-995-2696

Latin America: 877-919-9526

EMEA: +800 00200100 (Toll Free) or +1(650)385-2193

Asia Pacific: +65 6240 8484

Web: https://businessportal2.alcatel-lucent.com

Email: ebg_global_supportcenter@al-enterprise.com

Contents

About This Guide xxxv

Supported Platforms xxxv

Who Should Read this Manual? xxxvi

When Should I Read this Manual? xxxvi

What is in this Manual? xxxvi

What is Not in this Manual? xxxvii

How is the Information Organized? xxxvii

Text Conventions xxxvii

Documentation Roadmap xxxix

Related Documentation xl

Product Documentation xli

Technical Support xli

Chapter 1 **CMM Commands** 1-1

reload 1-2
reload working 1-4
copy running-config working 1-6
write memory 1-8
copy working certified 1-10
copy flash-synchro 1-12
takeover 1-13
show running-directory 1-15
show reload 1-17
show microcode 1-18
usb 1-20
usb auto-copy 1-21
usb disaster-recovery 1-23
mount 1-24
umount 1-25
show usb statistics 1-26
image integrity-check 1-28

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

system contact 2-3
system name 2-4
system location 2-5
system date 2-6
system time 2-7
system time-and-date synchro 2-8

system timezone 2-9
system daylight savings time 2-12
update 2-14
update lanpower 2-16
reload ni 2-17
reload all 2-18
reload pass-through 2-20
power ni 2-22
temp-threshold 2-23
stack set slot 2-24
stack set slot mode 2-26
stack clear slot 2-28
hash-control mode fdb 2-30
hash-control load-balance non-ucast 2-31
show system 2-32
show hardware info 2-34
show chassis 2-36
show cmm 2-38
show ni 2-41
show module 2-43
show module long 2-45
show module status 2-47
show power 2-49
show fan 2-51
show temperature 2-53
show stack topology 2-55
show stack status 2-58
show stack mode 2-59
show hash-control 2-61
show system hardware-self-test 2-63
show system process-self-test 2-64
license apply 2-65
license remove 2-66
license unlock 2-67
show license info 2-68
show license file 2-70
stack split-protection 2-72
stack split-protection linkaggid 2-73
stack split-protection guard-timer 2-74
stack split-protection helper 2-75
stack split-protection helper linkagg 2-76
show stack split-protection status 2-77
show stack split-protection statistics 2-78
show stack split-protection stacking-units 2-79
show stack split-protection helper status 2-80

Chapter 3 Chassis MAC Server (CMS) Commands 3-1
mac-range eeprom 3-2
mac-retention status 3-4
mac-retention dup-mac-trap 3-5
mac release 3-6
show mac-range 3-7

show mac-range alloc 3-9
show mac-retention status 3-11

Chapter 4 Power over Ethernet (PoE) Commands 4-1
lanpower start 4-3
lanpower delayed-start 4-5
lanpower stop 4-7
lanpower power 4-8
lanpower maxpower 4-10
lanpower priority 4-12
lanpower priority-disconnect 4-14
lanpower combo-port 4-16
lanpower high-resistance-detection 4-17
lanpower capacitor-detection 4-19
show lanpower 4-20
show lanpower delayed-start 4-23
show lanpower capacitor-detection 4-24
show lanpower priority-disconnect 4-25
show lanpower high-resistance-detection 4-26

Chapter 5 Network Time Protocol Commands 5-1
ntp server 5-2
ntp server synchronized 5-5
ntp server unsynchronized 5-6
ntp client 5-7
ntp broadcast 5-8
ntp broadcast-delay 5-9
ntp key 5-10
ntp key load 5-12
show ntp client 5-13
show ntp client server-list 5-15
show ntp server status 5-17
show ntp keys 5-20

Chapter 6 Session Management Commands 6-1
session login-attempt 6-3
session login-timeout 6-4
session banner 6-5
session timeout 6-7
session prompt default 6-8
session console 6-10
session xon-xoff 6-12
session cli-auto-complete-space 6-13
prompt 6-14
show prefix 6-16
alias 6-17
show alias 6-19
user profile save 6-20
user profile save global-profile 6-21
user profile reset 6-23
history size 6-24
show history 6-25

! 6-27
command-log 6-29
kill 6-30
exit 6-31
whoami 6-32
who 6-34
show session config 6-37
show session xon-xoff 6-39
more size 6-40
more 6-41
show more 6-42
telnet 6-43
telnet6 6-45
ssh 6-47
ssh6 6-49
ssh enforce pubkey-auth 6-51
show ssh config 6-52
show command-log 6-54
show command-log status 6-56

Chapter 7 File Management Commands 7-1
cd 7-3
pwd 7-5
mkdir 7-6
rmdir 7-8
ls 7-10
dir 7-12
rename 7-14
rm 7-16
delete 7-17
cp 7-18
scp 7-20
mv 7-22
move 7-24
chmod 7-26
attrib 7-27
freespace 7-28
fsck 7-29
newfs 7-31
rcp 7-32
rrm 7-33
rls 7-34
vi 7-36
view 7-37
tty 7-38
show tty 7-40
more 7-41
ftp 7-43
ftp6 7-45
scp-sftp 7-47
show ssh config 7-48
sftp 7-50

sftp6 7-52
tftp 7-54
rz 7-56

Chapter 8 Web Management Commands 8-1
http server 8-2
http ssl 8-3
http port 8-4
https port 8-5
debug http sessiondb 8-6
show http 8-8
webview wlan cluster-virtual-ip 8-10
webview wlan cluster-virtual-ip precedence 8-11
show webview wlan config 8-13

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

Chapter 10 SNMP and OpenFlow Commands 10-1
snmp station 10-3
snmp source ip preferred 10-5
show snmp station 10-6
snmp community map 10-8
snmp community map mode 10-10
show snmp community map 10-11
snmp security 10-12
show snmp security 10-14
show snmp statistics 10-16
show snmp mib family 10-18
snmp trap absorption 10-20
snmp trap to webview 10-21
snmp trap replay 10-22
snmp trap filter 10-24
snmp authentication trap 10-26
show snmp trap replay 10-27
show snmp trap filter 10-29
show snmp authentication trap 10-31
show snmp trap config 10-32
snmp view oid-tree 10-34
show snmp views 10-36
show snmp view viewname 10-38
openflow back-off-max 10-40
openflow idle-probe-timeout 10-41
openflow logical-switch 10-42
openflow logical-switch controller 10-44

openflow logical-switch interfaces 10-46
show openflow 10-47
show openflow logical-switch 10-48
show openflow logical-switch stats 10-50

Chapter 11 DNS Commands 11-1
ip domain-lookup 11-2
ip name-server 11-3
ipv6 name-server 11-5
ip domain-name 11-7
show dns 11-8

Chapter 12 Link Aggregation Commands 12-1
static linkagg size 12-3
static linkagg name 12-5
static linkagg admin state 12-6
static agg agg num 12-7
lacp linkagg size 12-9
lacp linkagg name 12-12
lacp linkagg admin state 12-13
lacp linkagg actor admin key 12-15
lacp linkagg actor system priority 12-16
lacp linkagg actor system id 12-17
lacp linkagg partner system id 12-18
lacp linkagg partner system priority 12-20
lacp linkagg partner admin key 12-21
lacp agg actor admin key 12-22
lacp agg actor admin state 12-25
lacp agg actor system id 12-27
lacp agg actor system priority 12-29
lacp agg partner admin state 12-31
lacp agg partner admin system id 12-33
lacp agg partner admin key 12-35
lacp agg partner admin system priority 12-37
lacp agg actor port priority 12-39
lacp agg partner admin port 12-41
lacp agg partner admin port priority 12-43
show linkagg 12-45
show linkagg port 12-50
show linkagg accounting 12-55
show linkagg counters 12-57
show linkagg traffic 12-60
linkagg no l2-statistics 12-62
dhl num 12-63
dhl num linka linkb 12-65
dhl num admin-state 12-67
dhl num vlan-map linkb 12-68
dhl num pre-emption-time 12-70
dhl num mac-flushing 12-72
show dhl 12-74
show dhl num 12-76
show dhl num link 12-79

Chapter 13 802.1AB Commands 13-1
lldp destination mac-address 13-3
lldp transmit fast-start-count 13-4
lldp transmit interval 13-5
lldp transmit hold-multiplier 13-6
lldp transmit delay 13-7
lldp reinit delay 13-8
lldp notification interval 13-9
lldp lldpdu 13-10
lldp notification 13-12
lldp network-policy 13-14
lldp med network-policy 13-16
lldp tlv management 13-18
lldp tlv dot1 13-20
lldp tlv dot3 mac-phy 13-22
lldp tlv dot3 power-via-mdi 13-24
lldp tlv med 13-26
lldp tlv proprietary 13-28
show lldp config 13-30
show lldp network-policy 13-32
show lldp med network-policy 13-34
show lldp system-statistics 13-36
show lldp statistics 13-38
show lldp local-system 13-40
show lldp local-port 13-43
show lldp local-management-address 13-46
show lldp remote-system 13-47
show lldp remote-system med 13-49
lldp trust-agent 13-52
lldp trust-agent violation-action 13-54
show lldp trusted remote-agent 13-56
show lldp trust-agent 13-58

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

Chapter 15 802.1Q Commands 15-1
vlan 802.1q 15-2
vlan 802.1q frame type 15-4
show 802.1q 15-5

Chapter 16 Distributed Spanning Tree Commands 16-1
bridge mode 16-4
bridge protocol 16-6
bridge cist protocol 16-8
bridge 1x1 protocol 16-10
bridge mst region name 16-12
bridge mst region revision level 16-14
bridge mst region max hops 16-15

bridge msti 16-17
bridge msti vlan 16-19
bridge priority 16-21
bridge cist priority 16-23
bridge msti priority 16-25
bridge 1x1 priority 16-27
bridge hello time 16-29
bridge cist hello time 16-31
bridge 1x1 hello time 16-33
bridge max age 16-35
bridge cist max age 16-37
bridge 1x1 max age 16-39
bridge forward delay 16-41
bridge cist forward delay 16-43
bridge 1x1 forward delay 16-45
bridge bpdu-switching 16-47
bridge path cost mode 16-49
bridge auto-vlan-containment 16-51
bridge slot/port 16-53
bridge cist slot/port 16-55
bridge 1x1 slot/port 16-57
bridge slot/port priority 16-59
bridge cist slot/port priority 16-61
bridge msti slot/port priority 16-63
bridge 1x1 slot/port priority 16-65
bridge slot/port path cost 16-67
bridge cist slot/port path cost 16-71
bridge msti slot/port path cost 16-75
bridge 1x1 slot/port path cost 16-78
bridge slot/port mode 16-81
bridge cist slot/port mode 16-83
bridge 1x1 slot/port mode 16-85
bridge slot/port connection 16-87
bridge cist slot/port connection 16-89
bridge 1x1 slot/port connection 16-91
bridge cist slot/port admin-edge 16-93
bridge 1x1 slot/port admin-edge 16-95
bridge cist slot/port auto-edge 16-97
bridge 1x1 slot/port auto-edge 16-99
bridge cist slot/port restricted-role 16-101
bridge 1x1 slot/port restricted-role 16-103
bridge cist slot/port restricted-tcn 16-105
bridge 1x1 slot/port restricted-tcn 16-107
bridge cist txholdcount 16-109
bridge 1x1 txholdcount 16-110
bridge rrstp 16-111
bridge rrstp ring 16-112
bridge rrstp ring vlan-tag 16-114
bridge rrstp ring status 16-116
show spantree 16-117
show spantree mode 16-123
show spantree cist 16-125

show spantree msti 16-129
show spantree 1x1 16-134
show spantree ports 16-138
show spantree cist ports 16-147
show spantree msti ports 16-151
show spantree 1x1 ports 16-157
show spantree mst region 16-163
show spantree msti vlan-map 16-165
show spantree cist vlan-map 16-167
show spantree map-msti 16-169
show spantree mst port 16-170
show bridge rrstp configuration 16-172
show bridge rrstp ring 16-173
bridge mode 1x1 pvst+ 16-175
bridge port pvst+ 16-176

Chapter 17 Ethernet Ring Protection Commands 17-1
erp-ring 17-2
erp-ring sub-ring-port 17-5
erp-ring protected-vlan 17-7
erp-ring rpl-node 17-9
erp-ring wait-to-restore 17-11
erp-ring enable 17-12
erp-ring ethoam-event remote-endpoint 17-13
erp-ring guard-timer 17-15
erp-ring virtual-channel 17-16
erp-ring revertive 17-18
erp-ring reset-version-fallback 17-20
erp-ring clear 17-21
clear erp statistics 17-22
show erp 17-24
show erp protected-vlan 17-27
show erp statistics 17-29

Chapter 18 Loopback Detection Commands 18-1
loopback-detection 18-2
loopback-detection port 18-3
loopback-detection transmission-timer 18-5
loopback-detection autorecovery-timer 18-6
show loopback-detection 18-7
show loopback-detection port 18-9
show loopback-detection statistics port 18-11

Chapter 19 CPE Test Head Commands 19-1
test-oam 19-3
test-oam direction 19-5
test-oam src-endpoint dst-endpoint 19-6
test-oam port 19-8
test-oam vlan test-frame 19-10
test-oam role 19-12
test-oam duration rate packet-size 19-14
test-oam frame 19-16

test-oam l2-saa 19-18
test-oam start stop 19-20
test-oam remote-sys-mac 19-22
test-oam statistics flash-logging 19-23
show test-oam 19-24
show test-oam statistics 19-28
show test-oam saa statistics 19-30
clear test-oam statistics 19-32
test-oam group 19-33
test-oam group tests 19-35
test-oam feeder 19-37
test-oam group src-endpoint dst-endpoint 19-38
test-oam group role 19-40
test-oam group port 19-42
test-oam group direction 19-44
test-oam group duration rate 19-46
test-oam group start stop 19-48
test-oam group remote-sys-mac 19-50
clear test-oam group statistics 19-51
show test-oam group 19-53
show test-oam group saa statistics 19-57
show test-oam group statistics 19-59

Chapter 20 Source Learning Commands 20-1
mac-address-table 20-2
mac-address-table static-multicast 20-4
mac-address-table aging-time 20-7
source-learning 20-9
hash-control chain-length 20-11
show hash-control chain-length 20-12
show mac-address-table 20-14
show mac-address-table static-multicast 20-17
show mac-address-table count 20-20
show mac-address-table aging-time 20-22
show source-learning 20-23

Chapter 21 PPPoE Intermediate Agent 21-1
pppoe-ia 21-2
pppoe-ia {port | linkagg} 21-4
pppoe-ia {trust | client} 21-6
pppoe-ia access-node-id 21-8
pppoe-ia circuit-id 21-10
pppoe-ia remote-id 21-13
clear pppoe-ia statistics 21-15
show pppoe-ia configuration 21-17
show pppoe-ia {port | linkagg} 21-20
show pppoe-ia statistics 21-23

Chapter 22 Learned Port Security Commands 22-1
port-security 22-2
port-security shutdown 22-4
port-security maximum 22-8

port-security max-filtering 22-10
port-security convert-to-static 22-12
port-security mac 22-14
port-security mac-range 22-16
port-security violation 22-19
port-security release 22-21
port-security learn-trap-threshold 22-23
show port-security 22-25
show port-security shutdown 22-29
show port-security brief 22-31

Chapter 23 Ethernet Port Commands 23-1
trap port link 23-4
interfaces speed 23-6
interfaces autoneg 23-8
interfaces crossover 23-10
interfaces pause 23-12
interfaces duplex 23-14
interfaces admin 23-16
interfaces alias 23-17
interfaces ifg 23-18
interfaces no l2 statistics 23-19
interfaces max frame 23-21
interfaces flood enable 23-22
interfaces flood rate 23-24
interfaces clear-violation-all 23-26
interfaces hybrid autoneg 23-27
interfaces hybrid crossover 23-29
interfaces hybrid duplex 23-31
interfaces hybrid speed 23-33
interfaces hybrid pause 23-35
interfaces tdr-test-start 23-37
interfaces no tdr-statistics 23-39
interfaces tdr-extended-test-start 23-40
interfaces no tdr-extended-statistics 23-42
interfaces transceiver ddm 23-43
interfaces eee 23-45
interfaces ptp 23-47
show interfaces 23-49
show interfaces tdr-statistics 23-54
show interfaces tdr-extended-statistics 23-58
show interfaces capability 23-60
show interfaces flow control 23-62
show interfaces pause 23-64
show interfaces accounting 23-66
show interfaces counters 23-69
show interfaces counters errors 23-72
show interfaces collisions 23-74
show interfaces status 23-76
show interfaces port 23-79
show interfaces ifg 23-82
show interfaces flood rate 23-84

show interfaces traffic 23-86
show interfaces hybrid 23-88
show interfaces hybrid status 23-92
show interfaces hybrid flow control 23-94
show interfaces hybrid pause 23-96
show interfaces hybrid capability 23-98
show interfaces hybrid accounting 23-100
show interfaces hybrid counters 23-102
show interfaces hybrid counters errors 23-104
show interfaces hybrid collisions 23-106
show interfaces hybrid traffic 23-108
show interfaces hybrid port 23-110
show interfaces hybrid flood rate 23-112
show interfaces hybrid ifg 23-114
interfaces violation-recovery-time 23-116
interfaces violation-recovery-maximum 23-118
interfaces violation-recovery-trap 23-120
interfaces clear-violation-all 23-121
show interfaces violation-recovery 23-122
link-fault-propagation group 23-124
link-fault-propagation group admin-status 23-126
link-fault-propagation group source 23-127
link-fault-propagation group destination 23-129
link-fault-propagation group wait to shutdown 23-131
show link-fault-propagation group 23-132
show interfaces transceiver 23-134
show interfaces eee 23-137
show interfaces ptp 23-139
show interfaces ptp-statistics 23-140

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

Chapter 25 VLAN Management Commands 25-1
vlan 25-2
vlan stp 25-4
vlan mobile-tag 25-6

vlan port default 25-8
vlan source-learning 25-10
show vlan 25-12
show vlan port 25-15
show vlan router mac status 25-18
show vlan gvrp 25-20
show vlan ipmvlan 25-22

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

Chapter 27 MVRP Commands 27-1
vlan registration-mode 27-2
mvrp 27-4
mvrp port 27-5
mvrp linkagg 27-7
mvrp transparent-switching 27-9
mvrp maximum vlan 27-10
mvrp registration 27-11
mvrp applicant 27-13
mvrp timer join 27-15
mvrp timer leave 27-17
mvrp timer leaveall 27-19
mvrp timer periodic-timer 27-21
mvrp periodic-transmission 27-23
mvrp restrict-vlan-registration 27-25
mvrp restrict-vlan-advertisement 27-27
mvrp static-vlan-restrict 27-29
show mvrp configuration 27-31
show mvrp port 27-33
show mvrp linkagg 27-36
show mvrp timer 27-39
show mvrp statistics 27-42
show mvrp last-pdu-origin 27-45
show vlan registration-mode 27-47
show mvrp vlan-restrictions 27-48

show vlan mvrp 27-50
mvrp clear-statistics 27-52

Chapter 28 VLAN Stacking Commands 28-1
ethernet-service 28-3
ethernet-service custom-L2-protocol 28-6
ethernet-service source-learning 28-9
ethernet-service service-name 28-11
ethernet-service svlan nni 28-13
ethernet-service nni 28-15
ethernet-service sap 28-18
ethernet-service sap uni 28-20
ethernet-service sap cvlan 28-22
ethernet-service sap-profile 28-24
ethernet-service sap sap-profile 28-27
ethernet-service uni-profile 28-29
ethernet-service uni uni-profile 28-33
ethernet-service uni-profile custom-L2-protocol 28-35
ethernet-service mac-tunneling 28-37
ethernet-service untagged-cvlan-insert 28-38
ethernet-service sap uni untagged-cvlan 28-39
ethernet-service svlan mac-tunneling 28-40
show ethernet-service custom-L2-protocol 28-42
show ethernet-service mode 28-44
show ethernet-service vlan 28-45
show ethernet-service 28-47
show ethernet-service sap 28-50
show ethernet-service port 28-52
show ethernet-service nni 28-55
show ethernet-service nni l2pt-statistics 28-57
clear ethernet-service nni l2pt-statistics 28-59
show ethernet-service uni 28-61
show ethernet-service uni l2pt-statistics 28-63
clear ethernet-service uni l2pt-statistics 28-66
show ethernet-service uni-profile 28-68
show ethernet-service uni-profile l2pt- statistics 28-70
show ethernet-service untagged-cvlan-insert 28-73
clear ethernet-service uni-profile l2pt-statistics 28-74
show ethernet-service sap-profile 28-75
loopback-test 28-77
show loopback-test 28-81

Chapter 29 Ethernet OAM Commands 29-1
ethoam vlan 29-3
ethoam domain 29-5
ethoam domain mhf 29-7
ethoam domain id-permission 29-8
ethoam association 29-9
ethoam association mhf 29-11
ethoam association id-permission 29-13
ethoam association ccm-interval 29-15
ethoam association endpoint-list 29-17

ethoam association allowed-cvlan-list 29-19
clear ethoam statistics 29-21
ethoam default-domain level 29-22
ethoam default-domain mhf 29-23
ethoam default-domain id-permission 29-24
ethoam default-domain primary-vlan 29-25
ethoam endpoint 29-27
ethoam endpoint admin-state 29-29
ethoam endpoint ccm 29-31
ethoam endpoint priority 29-33
ethoam endpoint lowest-defect-priority 29-35
ethoam endpoint domain association direction 29-37
ethoam endpoint ctag-priority 29-39
ethoam loopback 29-41
ethoam linktrace 29-43
ethoam fault-alarm-time 29-45
ethoam fault-reset-time 29-47
ethoam one-way-delay 29-49
ethoam two-way-delay 29-51
clear ethoam 29-53
show ethoam 29-54
show ethoam domain 29-56
show ethoam domain association 29-58
show ethoam domain association end-point 29-60
show ethoam default-domain 29-63
show ethoam default-domain configuration 29-65
show ethoam remote-endpoint domain 29-66
show ethoam cfmstack 29-68
show ethoam linktrace-reply domain association endpoint tran-id 29-70
show ethoam linktrace-tran-id 29-73
show ethoam vlan 29-75
show ethoam statistics 29-76
show ethoam config-error 29-78
show ethoam one-way-delay 29-80
show ethoam two-way-delay 29-82

Chapter 30 Service Assurance Agent Commands 30-1
saa 30-3
saa type ip-ping 30-5
saa type mac-ping 30-7
saa type ethoam-loopback 30-10
saa type ethoam-two-way-delay 30-13
saa start 30-15
saa stop 30-17
saa jitter-calculation 30-19
show saa config 30-21
show saa 30-22
show saa type config 30-24
show saa statistics 30-28

Chapter 31 LINK OAM Commands 31-1
efm-oam 31-3

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

Chapter 32 UDLD Commands 32-1
udld 32-2
udld port 32-3
udld mode 32-4
udld probe-timer 32-6
udld echo-wait-timer 32-8
clear udld statistics port 32-10
interfaces clear-violation-all 32-11
show udld configuration 32-12
show udld configuration port 32-13
show udld statistics port 32-15
show udld neighbor port 32-17
show udld status port 32-19

Chapter 33 Port Mapping Commands 33-1
port mapping user-port network-port 33-2
port mapping 33-4
port mapping 33-6
port mapping dynamic-proxy-arp 33-8
show port mapping status 33-10
show port mapping 33-12

Chapter 34 IP Commands 34-1
ip interface 34-5
Ip interface cvlan 34-8
ip managed-interface 34-10
ip interface dhcp-client 34-13
ip router primary-address 34-16
ip router router-id 34-17
ip static-route 34-18

ip route-pref 34-20
ip default-ttl 34-22
ping 34-23
traceroute 34-26
ip directed-broadcast 34-28
ip directed-broadcast allow 34-30
ip directed-broadcast clear 34-32
ip service 34-33
ip tables 34-35
ip redist 34-36
ip access-list 34-38
ip access-list address 34-39
ip route-map action 34-41
ip route-map match ip address 34-43
ip route-map match ipv6 address 34-45
ip route-map match ip-nexthop 34-47
ip route-map match ipv6-nexthop 34-49
ip route-map match tag 34-51
ip route-map match ipv4-interface 34-53
ip route-map match ipv6-interface 34-55
ip route-map match metric 34-57
ip route-map set metric 34-59
ip route-map set tag 34-61
ip route-map set ip-nexthop 34-63
ip route-map set ipv6-nexthop 34-65
arp 34-67
clear arp-cache 34-69
ip dos arp-poison restricted-address 34-70
arp filter 34-71
clear arp filter 34-73
ip arp-limit default 34-74
ip arp-limit extend 34-75
icmp type 34-76
icmp unreachable 34-79
icmp echo 34-81
icmp timestamp 34-83
icmp addr-mask 34-85
icmp messages 34-87
twamp server 34-88
ip dos scan close-port-penalty 34-90
ip dos scan tcp open-port-penalty 34-91
ip dos scan udp open-port-penalty 34-92
ip dos scan threshold 34-93
ip dos trap 34-95
ip dos scan decay 34-96
show ip traffic 34-97
show ip interface 34-100
show ip interface cvlan 34-106
show ip managed-interface 34-107
show ip route 34-109
show ip route-pref 34-111
show ip redist 34-112

show ip access-list 34-114
show ip route-map 34-116
show ip router database 34-118
show ip config 34-120
show ip protocols 34-122
show ip service 34-124
show arp 34-126
show ip dynamic-proxy-arp 34-128
show arp filter 34-130
show icmp control 34-132
show icmp statistics 34-134
show twamp server info 34-136
show twamp server connections 34-138
show tcp statistics 34-140
show tcp ports 34-142
show udp statistics 34-144
show udp ports 34-145
show ip dos config 34-146
show ip dos statistics 34-148
show ip dos arp-poison 34-150

Chapter 35 IPv6 Commands 35-1
ipv6 interface 35-3
ipv6 address 35-6
ipv6 dad-check 35-8
ipv6 hop-limit 35-9
ipv6 pmtu-lifetime 35-10
ipv6 host 35-11
ipv6 neighbor stale-lifetime 35-12
ipv6 neighbor 35-13
ipv6 prefix 35-15
ipv6 route 35-17
ipv6 static-route 35-18
ipv6 route-pref 35-20
ipv6 ra-filter 35-21
ipv6 ra-filter clear counters 35-23
ping6 35-24
traceroute6 35-26
show ipv6 hosts 35-28
show ipv6 icmp statistics 35-29
show ipv6 interface 35-32
show ipv6 pmtu table 35-36
clear ipv6 pmtu table 35-38
show ipv6 neighbors 35-39
clear ipv6 neighbors 35-41
show ipv6 prefixes 35-42
show ipv6 routes 35-44
show ipv6 route-pref 35-46
show ipv6 router database 35-47
show ipv6 tcp ports 35-49
show ipv6 traffic 35-51
clear ipv6 traffic 35-54

show ipv6 udp ports 35-55
show ipv6 information 35-57
show ipv6 ra-filter vlan 35-59
show ipv6 ra-filter counters 35-60
ipv6 redist 35-61
ipv6 access-list 35-63
ipv6 access-list address 35-64
show ipv6 redist 35-66
show ipv6 access-list 35-68
ipv6 load rip 35-70
ipv6 rip status 35-71
ipv6 rip invalid-timer 35-72
ipv6 rip garbage-timer 35-73
ipv6 rip holddown-timer 35-74
ipv6 rip jitter 35-75
ipv6 rip route-tag 35-76
ipv6 rip update-interval 35-77
ipv6 rip triggered-sends 35-78
ipv6 rip interface 35-79
ipv6 rip interface metric 35-81
ipv6 rip interface recv-status 35-82
ipv6 rip interface send-status 35-83
ipv6 rip interface horizon 35-84
show ipv6 rip 35-85
show ipv6 rip interface 35-87
show ipv6 rip peer 35-90
show ipv6 rip routes 35-92

Chapter 36 RDP Commands 36-1
ip router-discovery 36-2
ip router-discovery interface 36-3
ip router-discovery interface advertisement-address 36-5
ip router-discovery interface max-advertisement-interval 36-7
ip router-discovery interface min-advertisement-interval 36-9
ip router-discovery interface advertisement-lifetime 36-11
ip router-discovery interface preference-level 36-13
show ip router-discovery 36-15
show ip router-discovery interface 36-17

Chapter 37 DHCP Relay Commands 37-1
ip helper address 37-4
ip helper address vlan 37-6
ip helper standard 37-8
ip helper avlan only 37-9
ip helper per-vlan only 37-11
ip helper forward delay 37-13
ip helper maximum hops 37-15
ip helper agent-information 37-17
ip helper agent-information policy 37-19
ip helper pxe-support 37-21
ip helper dhcp-snooping 37-22
ip helper dhcp-snooping trap-mode 37-23

ip helper dhcp-snooping mac-address verification 37-24
ip helper dhcp-snooping option-82 data-insertion 37-25
ip helper dhcp-snooping option-82 format 37-26
ip helper dhcp-snooping option-82 format ascii circuit-id 37-28
ip helper dhcp-snooping option-82 format ascii remote-id 37-30
ip helper dhcp-snooping bypass option-82-check 37-32
ip helper dhcp-snooping vlan 37-33
ip helper dhcp-snooping port 37-35
ip helper dhcp-snooping linkagg 37-37
ip helper dhcp-snooping port traffic-suppression 37-39
ip helper dhcp-snooping port ip-source-filter 37-41
ip helper dhcp-snooping binding 37-43
ip helper dhcp-snooping ip-source-filter 37-45
ip helper dhcp-snooping binding timeout 37-47
ip helper dhcp-snooping binding action 37-48
ip helper dhcp-snooping binding persistency 37-49
ip helper dhcp-snooping ip-source-filter arp-allow 37-50
ip helper dhcp-snooping clear violation-counters 37-51
ip helper dhcp-snooping clear global-counters 37-52
show ip helper dhcp-snooping global-counters 37-53
ip helper dhcp-snooping clear isf-log 37-56
show ip helper dhcp-snooping isf-log 37-57
ip helper boot-up 37-58
ip helper boot-up enable 37-60
ip udp relay 37-61
ip udp relay vlan 37-63
dhcp-server 37-65
dhcp-server restart 37-66
show dhcp-server leases 37-67
show dhcp-server statistics 37-69
clear dhcp-server statistics 37-77
show ip helper 37-78
show ip helper stats 37-83
show ip helper dhcp-snooping vlan 37-85
show ip helper dhcp-snooping port 37-87
show ip helper dhcp-snooping binding 37-89
show ip udp relay service 37-91
show ip udp relay statistics 37-93
show ip udp relay destination 37-95
show ip helper dhcp-snooping ip-source-filter 37-97
ipv6 helper address 37-100
ipv6 helper address vlan 37-102
ipv6 helper standard 37-104
ipv6 helper per-vlan only 37-105
ipv6 helper maximum hops 37-106
ipv6 helper dhcp-snooping 37-107
ipv6 helper dhcp-snooping vlan 37-108
ipv6 helper dhcp-snooping port 37-109
ipv6 helper dhcp-snooping linkagg 37-111
ipv6 helper dhcp-snooping binding 37-113
ipv6 helper dhcp-snooping binding timeout 37-114
ipv6 helper dhcp-snooping binding action 37-115

ipv6 helper dhcp-snooping binding persistency 37-116
ipv6 helper dhcp-snooping ip-source-filter 37-117
ipv6 helper interface-id prefix 37-119
ipv6 helper remote-id format 37-120
show ipv6 helper 37-122
show ipv6 helper stats 37-125
show ipv6 helper dhcp-snooping vlan 37-127
show ipv6 helper dhcp-snooping port 37-128
show ipv6 helper dhcp-snooping binding 37-130
show ipv6 helper dhcp-snooping ip-source-filter 37-132
show ipv6 helper dhcp-snooping ip-source-filter binding 37-134

Chapter 38 RMON Commands 38-1
rmon probes 38-2
show rmon probes 38-4
show rmon events 38-7

Chapter 39 RIP Commands 39-1
ip load rip 39-2
ip rip status 39-3
ip rip interface 39-4
ip rip interface status 39-6
ip rip interface metric 39-8
ip rip interface send-version 39-9
ip rip interface recv-version 39-11
ip rip force-holddowntimer 39-12
ip rip host-route 39-14
ip rip route-tag 39-15
ip rip interface auth-type 39-16
ip rip interface auth-key 39-17
ip rip update-interval 39-18
ip rip invalid-timer 39-19
ip rip garbage-timer 39-20
ip rip holddown-timer 39-21
show ip rip 39-22
show ip rip routes 39-24
show ip rip interface 39-27
show ip rip peer 39-29

Chapter 40 VRRP Commands 40-1
vrrp 40-3
vrrp address 40-5
vrrp track 40-6
vrrp track-association 40-8
vrrp trap 40-9
vrrp delay 40-10
vrrp interval 40-11
vrrp priority 40-13
vrrp preempt 40-15
vrrp all 40-17
vrrp set 40-19
vrrp group 40-21

vrrp group all 40-23
vrrp group set 40-25
vrrp group-association 40-27
vrrp3 40-29
vrrp3 address 40-32
vrrp3 trap 40-33
vrrp3 track-association 40-34
show vrrp 40-35
show vrrp statistics 40-38
show vrrp track 40-41
show vrrp track-association 40-43
show vrrp group 40-45
show vrrp group-association 40-47
show vrrp3 40-49
show vrrp3 statistics 40-52
show vrrp3 track-association 40-54

Chapter 41 Port Mirroring and Monitoring Commands 41-1
port mirroring source destination 41-2
port mirroring 41-5
port monitoring source 41-7
port monitoring 41-9
show port mirroring status 41-10
show port monitoring status 41-12
show port monitoring file 41-14

Chapter 42 Health Monitoring Commands 42-1
health threshold 42-2
health threshold port-trap 42-4
health interval 42-6
health statistics reset 42-7
show health threshold 42-8
show health threshold port-trap 42-10
show health interval 42-12
show health 42-13
show health all 42-15
show health slice 42-17

Chapter 43 sFlow Commands 43-1
sflow receiver 43-3
sflow sampler 43-5
sflow poller 43-7
show sflow agent 43-9
show sflow receiver 43-11
show sflow sampler 43-13
show sflow poller 43-15

Chapter 44 QoS Commands 44-1
qos 44-3
qos trust ports 44-5
qos default servicing mode 44-7
qos forward log 44-9

qos log console 44-10
qos log lines 44-11
qos log level 44-12
qos default bridged disposition 44-14
qos default multicast disposition 44-16
qos stats interval 44-17
qos nms priority 44-18
qos phones 44-20
qos user-port 44-22
qos dei 44-24
qos force-yellow-priority 44-26
qos force-yellow-802.1p 44-28
qos force-yellow-dscp 44-30
debug qos 44-32
debug qos internal 44-34
qos clear log 44-36
qos apply 44-37
qos revert 44-38
qos flush 44-39
qos reset 44-41
qos stats reset 44-42
qos port reset 44-43
qos port 44-44
qos port trusted 44-46
qos port servicing mode 44-48
qos port q maxbw 44-50
qos port maximum egress-bandwidth 44-52
qos port maximum ingress-bandwidth 44-54
qos port default 802.1p 44-56
qos port default dscp 44-58
qos port default classification 44-60
qos port dei 44-62
show qos port 44-64
show qos queue 44-67
show qos queue statistics 44-70
show qos slice 44-73
show qos log 44-75
show qos config 44-77
show qos statistics 44-80
qos register shared buffers 44-83
qos port register profile 44-84
show qos register 44-85

Chapter 45 QoS Policy Commands 45-1
policy rule 45-5
policy rule accounting 45-9
policy validity period 45-10
policy network group 45-13
policy service group 45-15
policy mac group 45-17
policy port group 45-19
policy vlan group 45-22

policy map group 45-24
policy service 45-26
policy service protocol 45-29
policy service source tcp port 45-31
policy service destination tcp port 45-33
policy service source udp port 45-35
policy service destination udp port 45-37
policy condition 45-39
policy condition source ip 45-43
policy condition source ipv6 45-45
policy condition destination ip 45-47
policy condition destination ipv6 45-49
policy condition multicast ip 45-51
policy condition source network group 45-53
policy condition destination network group 45-55
policy condition multicast network group 45-57
policy condition source ip port 45-59
policy condition destination ip port 45-61
policy condition source tcp port 45-63
policy condition destination tcp port 45-65
policy condition source udp port 45-67
policy condition destination udp port 45-69
policy condition ethertype 45-71
policy condition established 45-73
policy condition tcpflags 45-75
policy condition service 45-77
policy condition service group 45-78
policy condition icmptype 45-80
policy condition icmpcode 45-82
policy condition ip protocol 45-84
policy condition ipv6 45-86
policy condition tos 45-88
policy condition dscp 45-90
policy condition source mac 45-92
policy condition destination mac 45-94
policy condition source mac group 45-96
policy condition destination mac group 45-98
policy condition source vlan 45-100
policy condition source vlan group 45-102
policy condition destination vlan 45-104
policy condition 802.1p 45-106
policy condition source port 45-108
policy condition destination port 45-110
policy condition source port group 45-112
policy condition destination port group 45-114
policy action 45-116
policy list 45-120
policy action disposition 45-123
policy action shared 45-125
policy action priority 45-127
policy action maximum bandwidth 45-129
policy action maximum depth 45-131

policy action cir 45-133
policy action tos 45-135
policy action 802.1p 45-137
policy action dscp 45-139
policy action map 45-141
policy action permanent gateway ip 45-143
policy action port-disable 45-145
policy action redirect port 45-147
policy action redirect linkagg 45-149
policy action no-cache 45-151
policy action mirror 45-152
show policy classify 45-154
show policy classify source port 45-157
show policy classify destination port 45-159
show policy classify source mac 45-161
show policy classify destination mac 45-163
show policy classify source vlan 45-165
show policy classify destination vlan 45-166
show policy classify source interface type 45-167
show policy classify destination interface type 45-169
show policy classify 802.1p 45-171
show policy classify source ip 45-172
show policy classify destination ip 45-173
show policy classify multicast ip 45-174
show policy classify tos 45-176
show policy classify dscp 45-178
show policy classify ip protocol 45-180
show policy classify source ip port 45-181
show policy classify destination ip port 45-183
show policy network group 45-185
show policy service 45-187
show policy service group 45-189
show policy mac group 45-191
show policy port group 45-193
show policy vlan group 45-195
show policy map group 45-197
show policy action 45-199
show policy list 45-202
show policy condition 45-204
show active policy list 45-207
show active policy rule 45-209
show active policy rule accounting 45-212
show active policy list accounting details 45-214
show active policy rule meter-statistics 45-216
show policy rule 45-219
show policy validity period 45-222
policy action rewrite 45-224
qos nat timeout 45-225
show qos nat flows 45-226
show qos nat counters 45-228
qos nat flush 45-230

Chapter 46 Policy Server Commands 46-1
policy server load 46-2
policy server flush 46-3
policy server 46-4
show policy server 46-6
show policy server long 46-8
show policy server statistics 46-10
show policy server rules 46-12
show policy server events 46-14

Chapter 47 IP Multicast Switching Commands 47-1
ip multicast status 47-3
ip multicast flood-unknown 47-5
ip multicast dynamic-control drop-all status 47-7
ip multicast querier-forwarding 47-9
ip multicast version 47-11
ip multicast max-group 47-13
ip multicast vlan max-group 47-15
ip multicast port max-group 47-17
ip multicast static-neighbor 47-19
ip multicast static-neighbor fast-convergence 47-21
ip multicast static-querier 47-22
ip multicast static-group 47-24
ip multicast query-interval 47-26
ip multicast last-member-query-interval 47-28
ip multicast query-response-interval 47-30
ip multicast unsolicited-report-interval 47-32
ip multicast router-timeout 47-34
ip multicast source-timeout 47-36
ip multicast querying 47-38
ip multicast robustness 47-40
ip multicast spoofing 47-42
ip multicast zapping 47-44
ip multicast proxying 47-46
ip multicast star-g-mode status 47-48
ip multicast vlan star-g-mode status 47-50
ipv6 multicast status 47-52
ipv6 multicast querier-forwarding 47-54
ipv6 multicast version 47-56
ipv6 multicast max-group 47-58
ipv6 multicast vlan max-group 47-60
ipv6 multicast port max-group 47-62
ipv6 multicast static-neighbor 47-64
ipv6 multicast static-querier 47-66
ipv6 multicast static-group 47-68
ipv6 multicast query-interval 47-70
ipv6 multicast last-member-query-interval 47-72
ipv6 multicast query-response-interval 47-74
ipv6 multicast unsolicited-report-interval 47-76
ipv6 multicast router-timeout 47-78
ipv6 multicast source-timeout 47-80
ipv6 multicast querying 47-82

ipv6 multicast robustness 47-84
ipv6 multicast spoofing 47-86
ipv6 multicast zapping 47-88
ipv6 multicast proxying 47-90
show ip multicast 47-92
show ip multicast port 47-97
show ip multicast forward 47-100
show ip multicast neighbor 47-102
show ip multicast querier 47-104
show ip multicast group 47-106
show ip multicast source 47-108
show ipv6 multicast 47-110
show ipv6 multicast port 47-115
show ipv6 multicast forward 47-117
show ipv6 multicast neighbor 47-119
show ipv6 multicast querier 47-121
show ipv6 multicast group 47-123
show ipv6 multicast source 47-125

Chapter 48 IP Multicast VLAN Commands 48-1
vlan ipmvlan 48-2
vlan ipmvlan ctag 48-4
vlan ipmvlan address 48-6
vlan ipmvlan sender-port 48-8
vlan ipmvlan receiver-port 48-10
vlan svlan port translate ipmvlan 48-12
show vlan ipmvlan c-tag 48-14
show vlan ipmvlan address 48-15
show vlan ipmvlan port-config 48-17
show ipmvlan port-config 48-19
show vlan ipmvlan port-binding 48-21

Chapter 49 AAA Commands 49-1
aaa radius-server 49-5
aaa test-radius-server 49-10
aaa radius-health-check 49-12
aaa tacacs+-server 49-14
aaa tacacs command-authorization 49-17
aaa tacacs server-wait-time 49-19
aaa ldap-server 49-20
aaa ace-server clear 49-23
aaa authentication 49-24
aaa authentication default 49-27
aaa authentication 802.1x 49-29
aaa authentication mac 49-31
aaa accounting 802.1x 49-33
aaa accounting mac 49-35
aaa accounting session 49-37
aaa accounting command 49-39
user 49-41
password 49-47
user password-size min 49-49

user password-expiration 49-50
user password-policy cannot-contain-username 49-52
user password-policy min-uppercase 49-53
user password-policy min-lowercase 49-54
user password-policy min-digit 49-55
user password-policy min-nonalpha 49-56
user password-history 49-57
user password-min-age 49-58
user lockout-window 49-59
user lockout-threshold 49-61
user lockout-duration 49-63
user lockout unlock 49-65
aaa admin-logout 49-66
system common-criteria 49-68
show system common-criteria 49-69
aaa certificate update-ca-certificate 49-70
aaa certificate update-crl 49-71
aaa certificate generate-rsa-key key-file 49-72
aaa certificate generate-self-signed 49-73
aaa certificate view 49-75
aaa certificate delete 49-78
aaa certificate generate-csr 49-79
end-user profile 49-81
end-user profile port-list 49-83
end-user profile vlan-range 49-85
aaa user-network-profile 49-87
aaa classification-rule mac-address 49-91
aaa radius nas-identifier 49-93
aaa radius nas-ip-address 49-94
show aaa radius config 49-96
aaa classification-rule mac-address-range 49-98
aaa classification-rule ip-address 49-100
aaa classification-rule lldp med-endpoint 49-102
aaa byod white-list 49-104
aaa byod white-list no 49-105
aaa hic server-name 49-106
aaa hic allowed-name 49-108
aaa hic 49-110
aaa hic web-agent-url 49-112
aaa hic custom-proxy-port 49-113
aaa hic redundancy background-poll-interval 49-114
aaa hic server-failure mode 49-115
aaa hic server-failure policy user-network-profile change 49-116
show aaa server 49-118
show aaa radius-health-check config 49-125
show radius-server statistics 49-127
clear radius-server statistics 49-131
show aaa authentication 49-132
show aaa authentication 802.1x 49-134
show aaa authentication mac 49-136
show aaa accounting 802.1x 49-137
show aaa accounting mac 49-138

show aaa accounting 49-140
show user 49-142
show user password-size 49-146
show user password-expiration 49-147
show user password-policy 49-148
show user lockout-setting 49-150
debug command-info 49-152
debug end-user profile 49-154
show end-user profile 49-156
show aaa user-network-profile 49-158
show aaa classification-rule 49-160
show aaa hic 49-163
show aaa hic host 49-165
show aaa hic server 49-167
show aaa hic allowed 49-169
show aaa hic server-failure policy 49-171
show aaa-device all-users 49-173
show aaa-device supplicant-users 49-177
show aaa-device non-supplicant-users 49-180
show aaa-device captive-portal-users 49-183
show aaa priv hexa 49-186
aaa redirect-server 49-189
aaa redirect url 49-191
aaa port-bounce 49-192
aaa redirect pause-timer 49-194
aaa redirect proxy-server-port 49-195
show aaa redirect-server 49-196
show aaa redirect url-list 49-198
show aaa port-bounce status 49-200
show aaa redirect pause-timer 49-202
show byod host 49-203
show byod status 49-205
show aaa byod white-list ip-address 49-207
show aaa user-network-profile 49-208
mdns-relay 49-210
mdns-relay tunnel 49-211
zeroconf mdns admin-state 49-212
zeroconf ssdp admin-state 49-213
zeroconf mode 49-214
zeroconf responder-ip 49-216
zeroconf gateway-vlan-list 49-218
zeroconf access-vlan-list 49-219
show mdns-relay config 49-220
show zeroconf config 49-222
aaa switch-access mode 49-224
aaa switch-access ip-lockout-threshold 49-225
aaa switch-access banned-ip release 49-227
aaa switch-access priv-mask 49-228
aaa switch-access management-stations 49-230
aaa switch-access management-stations ip-address 49-232
show aaa switch-access mode 49-234
show aaa switch-access ip-lockout-threshold 49-235

show aaa switch-access banned-ip 49-236
show aaa switch-access priv-mask 49-237
show aaa switch-access management-stations 49-239

Chapter 50 802.1x Commands 50-1
802.1x 50-3
802.1x initialize 50-6
802.1x re-authenticate 50-7
802.1x supp-polling retry 50-8
802.1x supplicant policy authentication 50-10
802.1x non-supplicant policy authentication 50-13
802.1x captive-portal name 50-16
802.1x non-supplicant policy 50-17
802.1x policy default 50-19
802.1x captive-portal policy authentication 50-21
802.1x captive-portal session-limit 50-23
802.1x captive-portal inactivity-logout 50-25
802.1x captive-portal retry-count 50-26
802.1x captive-portal address 50-28
802.1x delay-learning 50-29
802.1x captive-portal proxy-server-url 50-30
802.1x captive-portal proxy-server-port 50-31
802.1x captive-portal dns-keyword-list 50-32
802.1x captive-portal success-redirect-url 50-34
802.1x captive-portal fail-redirect-url 50-36
802.1x auth-server-down 50-38
802.1x auth-server-down policy 50-39
802.1x auth-server-down re-authperiod 50-41
802.1x auth-server-down 50-42
802.1x auth-server-down policy 50-43
802.1x server-polling 50-45
802.1x trust-radius 50-46
802.1x non-supplicant session timeout 50-48
show 802.1x 50-50
show 802.1x users 50-54
show 802.1x ap-client-mac 50-56
show 802.1x statistics 50-58
show 802.1x device classification policies 50-60
show 802.1x captive-portal configuration 50-62
show 802.1x non-supplicant 50-64
show 802.1x auth-server-down 50-66
show 802.1x rate-limit 50-68
802.1x supplicant bypass 50-70
802.1x non-supplicant allow-eap 50-72
802.1x pass-through 50-74
show 802.1x captive-portal configuration 50-75

Chapter 51 Switch Logging Commands 51-1
swlog 51-2
swlog syslog-facility-id 51-3
swlog appid level 51-5
swlog remote command-log 51-8

swlog output 51-9
swlog output flash file-size 51-11
swlog clear 51-12
show log swlog 51-13
show swlog 51-16

Chapter 52 OmniVista Cirrus Commands 52-1
cloud-agent admin-state 52-2
show cloud-agent status 52-4
show cloud-agent vpn status 52-8

Appendix A Software License and Copyright Statements A-1

Alcatel License Agreement A-1
ALE USA, Inc. 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 6350 Series, and OmniSwitch 6450 Series.

Supported Platforms

This information in this guide applies to the following products:

- OmniSwitch 6450 Series
- OmniSwitch 6350 Series

Unsupported Platforms

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

- OmniSwitch 6250
- OmniSwitch 9000 Series
- OmniSwitch 6400 Series
- OmniSwitch 6600 Family
- OmniSwitch 6800 Family
- OmniSwitch 6850 Series
- OmniSwitch 6855 Series
- OmniSwitch (original version with no numeric model name)
- OmniSwitch 7700/7800
- OmniSwitch 8800
- 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 benefit from the material in this reference guide. However, advanced users who have already familiarized themselves with the OmniSwitch CLI commands 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 is found in the *OmniSwitch AOS Release 6 Switch Management Guide* and the *OmniSwitch AOS Release 6 Network Configuration Guide*. Once you are familiar with the procedures and base CLI commands in these configuration guides, see the guide to obtain detailed information on the individual commands.

What is in this Manual?

This reference guide includes information on every CLI command available in the switch. 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 is 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. Commands in a single chapter 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, and so on. 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, for example, **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 has to choose between one or more parameters. Example: **port mirroring {enable | disable}** Here, you have to 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 helps you at each stage of the configuration process. Under each stage, we point you to the manual or manuals that is helpful to you.

Stage 1: Gaining Familiarity with Basic Switch Functions

Pertinent Documentation: *Hardware Users Guide*
Switch Management Guide

Once you have your switch up and running, you begin to understand the 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 2: Integrating the Switch Into a Network

Pertinent Documentation: *Network Configuration Guide*

When you are ready to connect your switch to the network, you 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.

Anytime

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

Related Documentation

User manuals can be downloaded at following

https://businessportal2.alcatel-lucent.com

The following are the titles and descriptions of all the related OmniSwitch 6350, 6450 user manuals:

- *OmniSwitch 6350 Hardware Users Guide*

  Complete technical specifications and procedures for all OmniSwitch 6350 chassis, power supplies, and fans. Also includes comprehensive information on assembling and managing stacked configurations

- *OmniSwitch 6450 Hardware Users Guide*

  Complete technical specifications and procedures for all OmniSwitch 6450 chassis, power supplies, and fans. Also includes comprehensive information on assembling and managing stacked configurations.

  Complete technical specifications and procedures for all OmniSwitch 6350 chassis, power supplies, and fans. Also includes comprehensive information on assembling and managing stacked configurations.

- *OmniSwitch AOS Release 6 CLI Reference Guide*

  Complete reference to all CLI commands supported on the OmniSwitch 6450, 6350. 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 Transceivers Guide*

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

- *AOS Release 6.7.2 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.

- *Technical Tips, Field Notices*

  Includes information published by Alcatel-Lucent Enterprise's Customer Support group.

Product Documentation

All products are shipped with a Product Documentation Card that provides details for downloading documentation for all OmniSwitch and other Alcatel-Lucent Enterprise data products. All user guides for the OmniSwitch Series are included on the Alcatel-Lucent Enterprise public website. This website also includes user guides for other Alcatel-Lucent Enterprise products. The latest user guides can be found on our website at:

https://businessportal2.alcatel-lucent.com

Technical Support

An Alcatel-Lucent Enterprise service agreement brings your company the assurance of 7x24 no-excuses technical support. You will also receive regular software updates to maintain and maximize your Alcatel product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners. Additionally, with 24-hour-a-day access to Alcatel's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel's technical support, open a new case or access helpful release notes, technical bulletins, and manuals.

For more information on Alcatel-Lucent Enterprise Service Programs:

Web: https://businessportal2.alcatel-lucent.com

Email: ebg_global_supportcenter@al-enterprise.com.

Phone:

North America: 800-995-2696

Latin America: 877-919-9526

EMEA: +800 00200100 (Toll Free) or +1(650) 385-2193

Asia Pacific: +65 6240 8484

1 CMM Commands

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

MIB information for the CMM commands is as follows:

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

Filename: AlcatelIND1ConfigMgr.mib
Module: ALCATEL-IND1-CONFIG-MGR-MIB

A summary of available commands is listed here:

reload
reload working
copy running-config working
write memory
copy working certified
copy flash-synchro
takeover
show running-directory
show reload
show microcode
show usb statistics
usb
usb auto-copy
usb disaster-recovery
mount
umount
image integrity-check

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 results in a secondary takover.
in [*hours***:]** *minutes*	Optional syntax. Schedules a reload of the software to take effect in the specified minutes or hours and minutes within the next 24 hours.
at *hour*:*minute*	Optional syntax. Schedules a reload of the software to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes 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 6450, 6350

Usage Guidelines

- This command causes the specified CMM to reboot. If no CMM is specified, the primary CMM reboots.
- If a reload command is issued, and another reload is currently scheduled, a message appears informing the user of the next reload time and asks for confirmation to change to the new reload time.
- If the switch has a redundant CMM and the primary CMM is rebooted, the switch fails 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 stacked configuration consisting of 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 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 in 15:25
-> reload primary at 15:25 august 10
-> reload primary at 15:25 10 august
```

Release History

Release 6.6.1; command 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 continues 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 takes place on the following day.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 has to 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 stacked configuration, 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 6.6.1; command introduced.

Related Commands

reload	Reboots the CMM to its startup software configuration.

MIB Objects

```
chasControlModuleTable
   csEntPhysicalIndex
   chasControlActivateTimeout
```

copy running-config working

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

[configure] copy running-config working

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is used to copy the changes made using the CLI commands from the running configuration (RAM) to the working directory. A trap is raised to enforce a poll whenever a configuration file is saved. The configuration changes that are not committed are not detected by the switch until **write memory** or **copy running-config working** is applied.
- 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 is overwritten if the **takeover** command is executed after the **copy running-config working** or **write memory** commands, in an OmniSwitch set up with redundant CMMs.

Examples

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

Release History

Release 6.6.1; command 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 6450, 6350

Usage Guidelines

- This command is used to copy the changes made using the CLI commands from the running configuration (RAM) to the working directory. A trap is raised to enforce a poll whenever a configuration file is saved. The configuration changes that are not committed are not detected by the switch until **write memory** or **copy running-config working** is applied.
- This command is only valid if the switch is running from the working directory. Use the **show running-directory** command to check from where the switch is running.
- This command performs the same function as the **copy running-config working** command.
- When this command is issued, the current stack topology will be compared against the saved stack topology. If there is any difference, a warning will be issued about the possible configuration purge and a confirmation from the user is required to proceed.

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

Examples

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

Release History

Release 6.6.1; command introduced.
Release 6.7.2.R04; Stack topology change confirmation introduced.

Related Commands

copy running-config working	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

```
configManager
   configWriteMemory
   configSaveSucceededTrapReason
```

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 6450, 6350

Usage Guidelines

- This command is used to overwrite the contents of the certified directory with the contents of the working directory. This has to be done only 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 a stacked configuration, 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 fails and an error message is generated. Only image files, the boot.cfg file, and the certs.pem file has to be kept in the working directory.
- This command does 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 6.6.1; command 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 6450, 6350

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 stackable configuration, all switches in the stack are updated with the primary CMM files.

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

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

Syntax Definitions

with-fabric	Performs a complete CMM reload.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 (that is, 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.
- This command can also be used on the secondary CMM.
- If the switch is part of an a stackable configuration consisting of 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 is overwritten if the **takeover** command is executed after the **copy running-config working** or **write memory** commands, in an OmniSwitch set up with redundant CMMs. Refer to the "NIs Reload On Takeover" description on page 1-16 for more information on the **takeover** command and redundant management modules.

Examples

```
-> takeover
-> takeover with-fabric
```

Release History

Release 6.6.1; command 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 6450, 6350

Usage Guidelines

- Once a switch has booted and is running, it runs 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

```
-> show running-directory

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

output definitions

Running CMM	The CMM currently controlling the switch, either PRIMARY or SECONDARY.
CMM Mode	Displays whether the primary and secondary CMMs are synchronized. In the case that there is no secondary CMM, MONO-CMM-CHASSIS is shown.
Current CMM Slot	The slot number of the primary CMM.
Running Configuration	Where the switch is running from, either WORKING or CERTIFIED. A switch running from the certified directory is unable to manipulate files in the directory structure.

output definitions (continued)

Certify/Restore Status	Indicates if the CM has been certified (that is, 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 is 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 is 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 (for example, a VLAN is configured on several different interfaces), and *the changes are not saved via the* **write memory** command, the corresponding NIs are automatically reload if a management module takeover occurs. Data flow on the affected NIs is interrupted until the reload is complete. Note that the NIs reload whether or not the flash synchronization status shows SYNCHRONIZED. This is because the unsaved changes have occurred in the running configuration (that is, 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 (for example, 1 6 9 12). If the flash directories on the primary and secondary management modules are *not synchronized* (for example, a **copy flash-synchro** command has not been issued recently), all NIs are reloaded automatically if a management module takeover occurs. Data flow is interrupted on all NIs until the reload is complete.

Release History

Release 6.6.1; command 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 6450, 6350

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 occurs.
- If the **reload working** command was used, and a rollback timeout was set, the time the rollback occurs 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 6.6.1; command introduced.

Related Commands

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

MIB Objects

N/A

show microcode

Displays microcode versions installed on the switch.

show microcode [working | certified | loaded]

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no additional parameters are entered (that is, **working**, **certified**, or **loaded**), microcode information for the running configuration is 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 Base Software
Jos.img           6.1.1.403.R01    1828255 Alcatel OS
Jadvrout.img      6.1.1.403.R01    1359435 Alcatel Advanced Routing
```

output definitions

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

Release History

Release 6.6.1; command introduced.

Related Commands

show microcode	Displays microcode versions installed on the switch.

MIB Objects

N/A

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 6450, 6350

Usage Guidelines

- Must use an Alcatel-Lucent certified USB device.
- If an Alcatel-Lucent certified USB device is connected after enabling the USB interface, the device is automatically mounted as **/uflash**.
- Once mounted, common file and directory commands can be used for file management.

Examples

```
-> usb enable
-> cp /flash/working/boot.cfg /uflash/boot.cfg
-> ls /uflash
```

Release History

Release 6.6.3; command introduced.

Related Commands

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

MIB Objects

```
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 6450, 6350

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 enables all of the image files from the */uflash/6350/working* or */uflash/6450/working,*, 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 is disabled before rebooting the switch and must be re-enabled by the administrator for the next auto-copy process to execute. This prevents running the same auto-copy multiple times.

Examples

```
-> usb auto-copy enable
-> usb auto-copy disable
```

Release History

Release 6.6.3; command 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 6450, 6350

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 KFos.img file then the disaster-recovery operation begins. The disaster recovery operation formats the switch flash, copy all of the files from the */uflash/6350/certified* or */uflash/6450/certified* directory, based upon the platform performing the operation, to the */flash/certified* directory and reboot the switch.
- Disaster recovery has to be run on a standalone unit so that it does not affect any other units in a stack.

Examples

```
-> usb disaster-recovery enable
-> usb disaster-recovery disable
```

Release History

Release 6.6.3; command introduced.

Related Commands

usb	Enables access to the device connected to the USB interface.
show usb statistics	Displays the status USB setting and features.

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 6450, 6350

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 6.6.3; command 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 6450, 6350

Usage Guidelines

This command unmounts the USB drive and has to be used prior to unplugging the USB drive to prevent possible data corruption.

Examples

```
-> umount /uflash
```

Release History

Release 6.6.3; command 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 6450, 6350

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 6.6.3; command 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

NA

image integrity-check

This command is used to check the integrity of the image files in working or certified directory.

image integrity-check {working | certified} *filename*

Syntax Definitions

working	Specifies the working directory of the switch. Image integrity check will be performed only for microcode information present in the working directory.
certified	Specifies the certified directory of the switch. Image integrity check will be performed only for microcode information present in the certified directory.
filename	Name of the file in flash which has the hash value from the image, against which the calculated hash value need to be compared.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When this command is entered without the filename, the SHA256 hash of the image files in selected directory (working/certified) is calculated and displayed. It can be manually verified against the hash provided in the file.
- When the command is entered with the filename, the SHA256 hash is calculated on the individual image files in the selected directory (working/certified) and compared with the hash information in the file.
- Hash value for the images needs to be stored in the <*filename*> in the below format.
  KFsecu.img:AE02549EA4D793593AD676F8A49A6522F2C9F4E
  KFeni.img:7F95BE32F2F1CB12E31D635AFA873C149551F1EA

Example

```
-> image integrity-check working
HASH for  KFsecu.img      :  BC077D4A467CA0794E231A841342783793AE48E8

HASH for  KFeni.img       :  9E09B914CFCA80333F6405116ADB89DF76A025C4

HASH for  KFos.img        :  CD1C0743F1EEBF3480677D649F0748FB70FE3A11

HASH for  KFdiag.img      :  4CF2A1E394906D40E6DBE6817C66664322B4CAED

HASH for  KFbase.img      :  3955CDAA1C49DC50D0B52BE35DA2E5E0769C710D
```

```
-> Image integrity-check working hash.txt
Computing the HASH for image files  .....

Image integrity check success for KFsecu.img
Image integrity check success for KFeni.img
Image integrity check success for KFos.img
 Image integrity check success for KFdiag.img
Image integrity check success for KFbase.img
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

N/A

MIB Objects

```
systemServicesAction
systemServicesArg1
systemServicesArg2
```

2 Chassis Management and Monitoring Commands

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

Additional Information. Refer to your separate *Hardware 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 set slot mode** **stack clear slot** **hash-control mode fdb** **hash-control load-balance non-ucast**
Stack Split Detection Commands	**stack split-protection** **stack split-protection linkaggid** **stack split-protection guard-timer** **stack split-protection helper** **stack split-protection helper linkagg** **show stack split-protection status** **show stack split-protection statistics** **show stack split-protection stacking-units** **show stack split-protection helper status**
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 stack mode** **show hash-control** **show system hardware-self-test** **show system process-self-test**
Licensing Commands	**license apply** **license remove** **license unlock** **show license info** **show license file**

system contact

Specifies the administrative contact of the switch. 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 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

system name	Modifies the current system name of the switch.
system location	Specifies the current physical location of the switch.
show system	Displays the basic system information for the switch.

MIB Objects

```
system
   systemContact
```

system name

Modifies the current system name of the switch. 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 6350"**.

Defaults

By default, the system name is set to 'VxTarget'.

Platforms Supported

OmniSwitch 6450, 6350

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 "OmniSwitch 6350"
-> system name OS-6350
```

Release History

Release 6.6.1; command introduced.

Related Commands

system contact	Specifies the administrative contact details of the switch (for example, an individual or a department).
system location	Specifies the current physical location of the switch.
show system	Displays the basic system information for the switch.

MIB Objects

```
system
   systemName
```

system location

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

system location *text_string*

Syntax Definitions

text_string	The physical location of the switch. 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 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; command introduced

Related Commands

system contact	Specifies the administrative contact of the switch (for example, an individual or a department).
system name	Modifies the current system name of the switch.
show system	Displays the basic system information for the switch.

MIB Objects

```
system
   systemLocation
```

system date

Displays or modifies the current system date of the switch.

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 6450, 6350

Usage Guidelines

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

Examples

```
-> system date 02/28/2017
```

Release History

Release 6.6.1; command introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesDate
```

system time

Displays or modifies the current system time of the switch.

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 6450, 6350

Usage Guidelines

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

Examples

```
-> system time 14:30:00
```

Release History

Release 6.6.1; command introduced.

Related Commands

system date	Displays or modifies the current system date of the switch.
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 Chassis Management Module (CMM).

system time-and-date synchro

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 refer to “Managing Stacks” in addition to “Managing CMM Directory Content” in the *OmniSwitch AOS Release 6 Switch Management Guide*.

Examples

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

Release History

Release 6.6.1; command 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 or GMT. Refer to the table in the "Usage Guidelines" section for a list of supported time zones. If you specify a time zone abbreviation, the hours offset from UTC is automatically calculated by the switch.
offset_value	Specifies the number of hours offset from UTC. Values can range from -13 through +12. The switch automatically enables UTC. If you do not want your system clock to run on UTC, enter the offset value as '+0'. This sets UTC to run on the 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

By default, the timezone is set to 'GMT'.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- To view the current time zone for the switch, enter the command **system timezone**.
- If Daylight Saving Time (DST), also referred to as *summertime*, is enabled, the clock automatically sets the default DST parameters for the local time zone. See "system daylight savings time" on page 2-12
- The OmniSwitch can be configured with a DHCP Client interface that allows the switch to dynamically obtain the time zone (DHCP Option-2) from a DHCP server. The user-defined time zone 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*.
- Refer to the following table 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

Abbreviation	Name	Hours from UTC	DST Start	DST End	DST Change
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
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 6.6.1; command introduced.

Related Commands

system date	Displays or modifies the current system date of the switch.
system time	Displays or modifies the current system time of the switch.

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 automatically adjusts for DST as specified by one of the default time zones or by the specifications set with the system daylight savings time start command.
disable	Disables DST. The switch clock does not change for DST.
start	For non-default time zone, specify the *week*, *day*, *month*, and *hour* for DST to start. (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 have to 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 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 offsets one hour for DST.

Platforms Supported

OmniSwitch 6450, 6350

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 automatically adjusts for DST as shown in the table.
- You must enable DST whether you use a default DST timezone or if you specify your offset using the **daylight savings time start** syntax.

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

system time	Displays or modifies the current system time of the switch.
system timezone	Displays or modifies the timezone for the switch.
system date	Displays or modifies the current system date of the switch.

MIB Objects

```
systemServices
   systemServicesTimezone
   systemServicesEnableDST
```

update

Updates the versions of Uboot, FPGA, BootROM, or Miniboot. Refer to the Release Notes and 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.
ni	Specifies that the update is performed for the 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 on all available switches within a stack.
miniboot	Updates the miniboot version.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- 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 can affect 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:

Platform	Update Type	Update File
OmniSwitch 6450, 6350	Uboot	kfu-boot.bin
	Miniboot	kfminiboot.bs
	Uboot and Miniboot	kfu-boot.bin kfminiboot.bs
	FPGA	KFfpga.upgrade_kit

Examples

```
-> update uboot 2
-> update uboot-miniboot
-> update fpga cmm
-> update miniboot 3
```

Release History

Release 6.6.1; command introduced.

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. Contact Alcatel 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> update lanpower 3
-> update lanpower all
```

Release History

Release 6.6.1; command introduced.

Related Commands

update	Updates the versions of Uboot, FPGA, BootROM, or Miniboot.

reload ni

Reloads (that is, reboots) a specified 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 6450, 6350

Usage Guidelines

The **reload ni** command reboots only the specified switch. 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 6.6.1; command 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 NI module.
show ni	Shows the hardware information and the status for NI modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   reset
```

reload all

Reloads all NIs and CMMs.

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, reload takes place at the specified time on the current day provided the specified time is later than the time the CLI command was issued. If the specified time is earlier than the current time, the reload takes 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.
cancel	Cancels a pending time delayed reload.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> reload all
```

Release History

Release 6.6.1; command introduced.

Related Commands

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

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   reset
```

reload pass-through

Reloads a switch in a stacked configuration that has been forced into the pass-through mode. The pass-through mode is a state in which a switch is 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 (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 (stack) is not 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.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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, and so on.
- 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 assumes after it has been rebooted. If the saved slot number is not unique, the switch returns 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 6.6.1; command 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 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 6450, 6350

Usage Guidelines

Use the **no** form of this command to power off the corresponding switch in a stacked configuration.

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

reload ni	Reloads a specified NI module.
show ni	Shows the hardware information and status for NI modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable
   chasEntPhysAdminStatus
   powerOn
   powerOff
```

temp-threshold

Sets the CPU 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 CPU warning temperature threshold is set.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use the **show temperature** command to display the current value for the temperature 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 6.6.1; command introduced.

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 for a switch in a stacked configuration. The saved slot number is the slot position the switch assumes following a reboot. The **stack set slot** command also provides syntax for immediately rebooting the corresponding switch.

stack set slot *slot-number* **saved-slot** *saved-slot-number* **[reload]**

Syntax Definitions

slot-number	The current slot position used by the switch (1–8; 1001–1008). The valid slot number range also includes slot positions 1001 through 1008, reserved for switches in pass-through mode.
saved-slot-number	The new (that is, saved) slot number (1–8). The saved slot number is the slot position the switch assumes 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 reboots immediately and the new (saved) slot number takes effect when the switch comes back up barring any pass-though mode conditions, such as duplicate slot numbers.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 /flash directory of the switch and is used when assigning a slot number for the switch during the boot process.
- To avoid duplicate slot numbers within the virtual chassis (that 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*.
- In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> stack set slot 2 saved-slot 3
-> stack set slot 1001 saved-slot 4 reload
```

Release History

Release 6.6.1; command introduced.

Related Commands

stack clear slot	Clears the current saved slot information for a switch within a stacked configuration.
show stack topology	Displays the current operating topology of switches within a stack.

MIB Objects

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrSavedSlotNINumber
   alaStackMgrCommandAction
   alaStackMgrCommandStatus
```

stack set slot mode

Sets the switch to either stackable or standalone mode. The **stack set slot mode** command also provides syntax for immediately rebooting the corresponding switch.

stack set slot *slot-number* **mode {stackable | standalone} [reload]**

Syntax Definitions

slot-number	The current slot position used by the switch (1–8; 1001–1008). The valid slot number range also includes slot positions 1001 through 1008, reserved for switches in pass-through mode.
stackable	Sets the switch to stackable mode allowing the switch to be stacked into a virtual chassis using the fixed fiber ports.
standalone	Sets the switch to standalone mode allowing the fixed fiber ports to be used as uplink ports.
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 reboots immediately and the new mode takes effect when the switch comes back up.

Defaults

parameter	default
mode	Standalone

Platforms Supported

OmniSwitch 6450-10, OmniSwitch 6350

Usage Guidelines

- Reboot the switch for the new mode to take effect.
- In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> stack set slot 2 mode stackable
```

Release History

Release 6.6.1; command introduced.
Release 6.6.4;command introduced on OS6450-10.

Related Commands

show stack mode	Displays the current mode of the switches.

MIB Objects

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrCommandAction
   alaStackMgrCommandStatus
```

stack clear slot

Clears the current saved slot information for a switch within a stacked configuration. When the saved slot information is cleared using the **stack clear slot** command, the corresponding switch is automatically assigned a unique slot number following a reboot. The command also provides optional syntax for immediately forcing the corresponding switch into pass-though mode.

stack clear slot *slot-number* **[immediate]**

Syntax Definitions

slot-number	The current slot position used by the switch (1–8; 1001–1008). The valid slot number range also includes slot positions 1001 through 1008, reserved for switches in pass-through mode.
immediate	Optional command syntax. When **immediate** is entered in the command line, the corresponding switch is manually forced into pass-through mode at the time the command is entered. All traffic on the Ethernet ports of the switch is stopped. Unprocessed traffic (if applicable) continue to pass through the stacking cables to other switches in the stack. A limited number of management commands on the switch are also supported.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When the **stack clear slot** command is issued, the **boot.slot.cfg** file is immediately removed from the /flash directory of the switch. As a result, no slot assignment information is found the next time the switch is booted. The switch is automatically assigned a unique slot number during the boot process.
- 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 reboots and assumes 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.
- In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> stack clear slot 1002
-> stack clear slot 3 immediate
```

Release History

Release 6.6.1; command introduced.

Related Commands

stack set slot	Sets the saved slot number for a switch in a stacked configuration.
show stack topology	Displays the current operating topology of switches within a stack.

MIB Objects

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrSavedSlotNINumber
   alaStackMgrCommandAction
   alaStackMgrCommandStatus
```

hash-control mode fdb

Configures the hash control method on the switch. Depending on this configuration, hashing algorithm used by various applications for Layer 2 table lookup is affected.

hash-control mode fdb { xor | crc }

Syntax Definitions

xor	Sets hash control lookup to XOR mode.
crc	Sets hashing to extended mode.

Defaults

parameter	default
fdb	xor

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The hash control setting impacts the fabric load balancing for chassis based products.
- Changing the hash control mode affects the hashing algorithm for Link Aggregation and EMCP.
- Changing the hash mode requires a switch or stack reboot.

Examples

```
-> hash-control mode fdb xor
-> hash-control mode fdb crc
```

Release History

Release 6.6.3; command introduced.

Related Commands

show hash-control	Displays the current hash control setting for the switch.

MIB Objects

```
alaChasHashMode
alachasFdbHashMode
```

hash-control load-balance non-ucast

Enable or disable the hashing for non-unicast traffic, which will load balance the non-unicast traffic across all ports in the linkagg at a global level.

hash-control load-balance non-ucast {enable | disable}

Syntax Definitions

enable	Enables load balance for non-unicast traffic.
disable	Disables load balance for non-unicast traffic.

Defaults

By default, hash control setting for non-unicast traffic is disabled.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

This command configures the hash control register in the hardware. Depending upon the configuration, hashing algorithm used by various applications for packet forwarding will be decided.

Examples

```
-> hash-control load-balance non-ucast enable
-> hash-control load-balance non-ucast disable
```

Release History

Release 6.7.2.R06; command introduced.

Related Commands

show hash-control	Displays the current hash control setting for the switch.

MIB Objects

```
alachasNonUCHashControl
```

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 6450, 6350

Usage Guidelines

This command can be used when logged in to the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show system
System:
Description:  Alcatel-Lucent OS6450-10 6.7.2.26.R01 Development, March 01, 2017.,
  Object ID:    1.3.6.1.4.1.6486.800.1.1.2.1.12.1.1,
  Up Time:      0 days 3 hours 7 minutes and 1 seconds,
  Contact:      Lab Admin,
  Name:         OS6450-10,
  Location:     NMS_LAB,
  Services:     72,
  Date & Time:  FRI MAR 03 2017  00:30:57 (UTC)

Flash Space:
    Primary CMM:
      Available (bytes):  47302656,
      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.

output definitions (continued)

System Name	A user-defined text description for the switch. This field is modified using the **system name** command.
System Location	The user-defined physical location of the switch. This field is modified using the **system location** command.
System Services	The number of current system services.
System Date & Time	The current system date and time. This field is modified using the **system date** and **system time** commands.
Flash Space: Primary CMM: Available (bytes)	The available flash memory space available on the *primary* management module of the switch.
Flash Space: Primary CMM: Comments	Comments regarding the available flash memory space available on the primary management module of the switch, if applicable.

Release History

Release 6.6.1; command introduced.

Related Commands

system contact	Specifies the administrative contact of the switch (for example, an individual or a department).
system name	Modifies the current system name of the switch.
system location	Specifies the current physical location of the switch.

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 6450, 6350

Usage Guidelines

This command can be used when logged in to the switch that performs either as the primary or secondary CMM role in a stack.

Examples

```
-> show hardware info
CPU Type                          : Marvell Feroceon,
Flash Manufacturer                : Micron Technology, Inc.,
Flash size                        : 134217728 bytes (128 MB),
RAM Manufacturer                  : Nanya Technology,
RAM size                          : 268435456 bytes (256 MB),
Miniboot Version                  : 6.6.3.259.R01,
Product ID Register               : 07
Hardware Revision Register        : 41
FPGA Revision Register            : 6
```

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.
Miniboot Version	The current default miniboot version.
Product ID Register	The register number of the product ID.

output definitions (continued)

Hardware Revision Register	The register number of the hardware revision.
FPGA Revision Register	The register number of the FPGA revision.

Release History

Release 6.6.1; command 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 6450, 6350

Usage Guidelines

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

Examples

```
-> show chassis

Chassis 1
  Model Name:                   OS6450-U24,
  Description:                  Chassis,
  Part Number:                  903175-90,
  Hardware Revision:            04,
  Serial Number:                P1180657,
  Manufacture Date:             MAR 14 2013,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Number Of Resets:             563
  MAC Address:                  xx:xx:xx:xx:xx:xx,

Chassis 2
  Model Name:                   OS6450-U24,
  Description:                  22 100/1000,
  Part Number:                  903038-90,
  Hardware Revision:            04,
  Serial Number:                M518025P,
  Manufacture Date:             DEC 28 2011,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  MAC Address:                  xx:xx:xx:xx:xx:xx,

Chassis 3
  Model Name:                   OS6450-P24,
  Description:                  24 POE 10/100/1000,
  Part Number:                  903174-90,
```

```
  Hardware Revision:            05,
  Serial Number:                P1381963,
  Manufacture Date:             APR 02 2013,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  MAC Address:                  xx:xx:xx:xx:xx:xx,

Chassis 4
  Model Name:                   OS6450-48,
  Description:                  48 10/100/1000,
  Part Number:                  903107-90,
  Hardware Revision:            01,
  Serial Number:                M428026P,
  Manufacture Date:             OCT 10 2011,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  MAC Address:                  xx:xx:xx:xx:xx:xx,
```

output definitions

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

Related Commands

show hardware info	Displays the current system hardware information.
show power	Displays the hardware information and 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 6450, 6350

Usage Guidelines

- A switch with a secondary CMM role in a stack also displays the hardware and the status information for the primary switch in the stack.
- This command can be used when logged in to the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show cmm
CMM in slot 1
  Model Name:                   OS6450-U24,
  Description:                  CMM,
  Part Number:                  903175-90,
  Hardware Revision:            04,
  Serial Number:                P1180657,
  Manufacture Date:             MAR 14 2013,
  Firmware Version:             n/a,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Consumption:            0,
  Power Control Checksum:       0xc398,
  CPU Model Type   :            MV88F6281 Rev 2,
  MAC Address:                  xx:xx:xx:xx:xx:xx,


CMM in slot 2
  Model Name:                   OS6450-U24,
  Description:                  CMM,
  Part Number:                  903038-90,
  Hardware Revision:            04,
  Serial Number:                M518025P,
  Manufacture Date:             DEC 28 2011,
```

```
Firmware Version:              n/a,
Admin Status:                  POWER ON,
Operational Status:            SECONDARY,
Power Consumption:             0,
Power Control Checksum:        0x42b2,
CPU Model Type   :             MV88F6281 Rev 2,
MAC Address:                   xx:xx:xx:xx:xx:xx,
```

output definitions

Model Name	The model name of the switch.
Description	A factory-defined description of the associated board (for example, BBUS Bridge, or PROCESSOR).
Part Number	The Alcatel part number for the board.
Hardware Revision	The hardware revision level for the board.
Serial Number	The Alcatel serial number for the board.
Manufacture Date	The date the board was manufactured.
Firmware Version	The firmware version for the ASIC of the board.
Admin Status	The current power status of the CMM. Admin status value is always POWER ON as the information is obtained from a running CMM.
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 does not change if the CMM is replaced or becomes secondary. The MAC address is used by the Chassis MAC Server (CMS) for allocation to various applications. Refer to the “Managing MAC Addresses and Ranges” chapter of the *OmniSwitch AOS Release 6 Switch Management Guide* for more information.

Release History

Release 6.6.1; command 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 basic system information for the switch.

MIB Objects

N/A

show ni

Displays the basic hardware and status information for 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 6450, 6350

Usage Guidelines

This command can be used when logged in to the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show ni 1

Module in slot 1
  Model Name:                   OS6450-U24,
  Description:                  22 100/1000,
  Part Number:                  903175-90,
  Hardware Revision:            04,
  Serial Number:                P1180657,
  Manufacture Date:             MAR 14 2013,
  Firmware Version:             ,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Consumption:            0,
  Power Control Checksum:       0xc398,
  CPU Model Type   :            ARM926 (Rev 1),
  MAC Address:                  xx:xx:xx:xx:xx:xx,
  ASIC - Physical 1:            MV88F6281 Rev 2,
  FPGA - Physical 1:            005/00,
  UBOOT Version :               n/a,
  UBOOT-miniboot Version :      6.7.1.54.R02,
  POE SW Version :              n/a
```

output definitions

Model Name	The module name of NI. 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 part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The Alcatel serial number for the printed circuit board (PCB) of the NI.
Manufacture Date	The date the NI was manufactured.
Firmware Version	The firmware version for the ASIC of the NI.
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 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 ASIC of the module.
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).

Release History

Release 6.6.1; command introduced.

Related Commands

reload ni	Reloads a specified NI module.
power ni	Turns the power on or off for a specified 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 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 6450, 6350

Usage Guidelines

This command can be used when logged in to 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    903175-90      P1180657     04  MAR 14 2013  OS6450-U24
CMM-2    903038-90      M518025P     04  DEC 28 2011  OS6450-U24
```

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 Users Guide*. Refer to page 2-38 for additional information on CMM location callouts.
Part-Number	The Alcatel part number for the module.
Serial #	The Alcatel serial number for the module.
Rev	The hardware revision level for the module.
Date	The date the module was manufactured.
Model Name	The descriptive name for the module. For example, OS9-GNI-U24 indicates a twenty four-port Gigabit Ethernet module.

Release History

Release 6.6.1; command 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.

MIB Objects

N/A

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 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 slot number is not specified, detailed information for all the modules is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When a particular NI module is specified in the command line, output is the same as that of the **show ni** command.
- This command can be used when logged in to the switch that performs either the primary or secondary CMM role in a stack.

Examples

```
-> show module long
CMM in slot 1
  Model Name:                   OS6450-U24,
  Description:                  CMM,
  Part Number:                  903175-90,
  Hardware Revision:            04,
  Serial Number:                P1180657,
  Manufacture Date:             MAR 14 2013,
  Firmware Version:             n/a,
  Admin Status:                 POWER ON,
  Operational Status:           UP,
  Power Consumption:            0,
  Power Control Checksum:       0xc398,
  CPU Model Type   :            MV88F6281 Rev 2,
  MAC Address:                  xx:xx:xx:xx:xx:xx,

Module in slot 1
  Model Name:                   OS6450-U24,
  Description:                  22 100/1000,
  Part Number:                  903175-90,
  Hardware Revision:            04,
  Serial Number:                P1180657,
```

```
Manufacture Date:              MAR 14 2013,
Firmware Version:              ,
Admin Status:                  POWER ON,
Operational Status:            UP,
Power Consumption:             0,
Power Control Checksum:        0xc398,
CPU Model Type   :             ARM926 (Rev 1),
MAC Address:                   xx:xx:xx:xx:xx:xx,
ASIC - Physical 1:             MV88F6281 Rev 2,
FPGA - Physical 1:             005/00,
UBOOT Version :                n/a,
UBOOT-miniboot Version :       6.7.1.54.R02,
POE SW Version :               n/a
```

output definitions

Model Name	The module name of NI. 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 part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The Alcatel serial number for the printed circuit board (PCB) of NI.
Manufacture Date	The date the NI was manufactured.
Firmware Version	The firmware version for ASIC of NI.
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 ASIC of NI.
CPLD - Physical	General information regarding the CPLD.

Release History

Release 6.6.1; command 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.

MIB Objects

N/A

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 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 6450, 6350

Usage Guidelines

This command can be used when logged in to 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     xx:xx:xx:xx:xx:xx
NI-1     UP           POWER ON      N/A     xx:xx:xx:xx:xx:xx
```

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 Users Guide*. Refer to page 2-38 for additional information on CMM callouts.
Operational Status	The operational status of the module. Options include UP or DOWN. For NI and secondary CMM modules, the operational status can be DOWN while the power status is on, indicating a possible software issue.
Admin-Status	The current power status of the module. Options include POWER ON or POWER OFF.

output definitions (continued)

Firmware Rev	The firmware version for module's ASICs.
MAC	For the CMM, the base chassis MAC address is displayed. For detailed information on this base chassis MAC address, refer to the "Managing MAC Addresses and Ranges" chapter of the *OmniSwitch AOS Release 6 Switch Management Guide*. For NI modules, the MAC address for the corresponding NI is displayed.

Release History

Release 6.6.1; command 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.

MIB Objects

N/A

show power

Displays the hardware information and 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 6450, 6350

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.

Examples

```
-> show power
Slot  PS   Wattage   Type   Status     Location
----+----+---------+------+-----------+----------
 1    1     530      AC    UP           Internal
 1    2     --       --    --           --
 2    1     530      AC    UP           Internal
 3    1     320      AC    UP           Internal
 4    1     600      AC    UP           External
```

output definitions

Slot	The slot number of the power supply.
PS	The power supply number.
Wattage	The wattage of the power supply.
Type	The type of power supply. Options include AC or DC.
Status	The operational status of the power supply. Options include UP or DOWN.
Location	The location of the power supply. Options include Internal or External.

Release History

Release 6.6.1; command introduced.

Related Commands

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

MIB Objects

N/A

show fan

Displays the current operating status of chassis fans.

show fan [*number***]**

Syntax Definitions

number	Specifies the switch (slot) number of the chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

This parameter specifies the switch (slot) number of the chassis. If no switch number is specified, then all the switches in a stack is displayed.

Examples

```
-> show fan
Chassis Fan  Status
-------+---+-----------
   1     1   Running
   1     2   Running
   1     3   Running
   1     4   Not Running
   1     5   Not Running
   1     6   Not Running
   2     1   Running
   2     2   Running
   2     3   Running
   2     4   Not Running
   2     5   Not Running
   2     6   Not Running
   3     1   Running
   3     2   Running
   3     3   Running
   3     4   Not Running
   3     5   Not Running
   3     6   Not 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 6.6.1; command introduced.

Related Commands

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

MIB Objects

N/A

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, temperature information for all switches operating in the stack is displayed by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The *number* parameter is not an option when using this command on a standalone switch.

Examples

```
-> show temperature

Temperature for chassis 1
  Hardware Board Temperature (deg C)              = 41,
  Hardware Cpu Temperature (deg C)                = N/A,
  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,
  Hardware Cpu Temperature (deg C)                = N/A,
  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,
  Hardware Cpu Temperature (deg C)                = N/A,
  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 Centigrade (Celsius). This temperature is checked against the upper threshold value. If the threshold is exceeded, a warning is sent to the user.
Hardware Cpu Temperature	The current CPU temperature. The temperature is displayed in degrees Centigrade (Celsius).
Temperature Upper Threshold Range	The supported threshold range. When you specify a threshold for the switch using 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 TEMP LED of the CMM 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 2-23.
Temperature Range	The current threshold status of the switch. Displays whether the switch is UNDER THRESHOLD or OVER THRESHOLD. If the status is OVER THRESHOLD, the primary TEMP LED of the CMM displays amber, and a warning is sent to the user.
Temperature Danger Threshold	The factory-defined danger threshold. This field is not configurable. If the chassis temperature rises above the danger threshold, the switch powers off all NI modules until the temperature conditions (for example, chassis air flow obstruction or ambient room temperature) is addressed and the switch is manually booted.

Release History

Release 6.6.1; command introduced.

Related Commands

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

MIB Objects

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

show stack topology

Displays the current operating topology of switches within a stack.

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

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

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 (stacked configuration). 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 assign these slot numbers, 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 current role of the switch is not known).
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 and has automatically entered pass-through mode), CLR-SLOT (the switch has been manually "cleared" through 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 current state of the switch is not known).
Saved Slot	The designated saved slot number for the corresponding switch. The saved slot number is the slot position the switch assumes 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 status of the stacking cable link at the stacking port A of the switch. Options include UP, DOWN, or UNKNOWN.
Link A Remote NI	The slot number of the switch to which *remote end* of the stacking cable A 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 *remote end* of the stacking cable A is connected. Options include StackA, StackB, and 0. If the remote end of the stacking cable A 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 status of the stacking cable link at the stacking port B of the switch. Options include UP, DOWN, or UNKNOWN.

output definitions (continued)

Link B Remote NI	The slot number of the switch to which *remote end* of the stacking cable B 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 *remote end* of the stacking cable B is connected. Options include StackA, StackB, and 0. If the remote end of the stacking cable B is connected to stacking port B on the other switch, the value displays StackB. If there are no stacking cable links, the value 0 displays.

Release History

Release 6.6.1; command introduced.

Related Commands

show stack status	Displays the current redundant stacking cable status and token availability for a stacked configuration.

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 6450, 6350

Usage Guidelines

In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> show stack status

Redundant cable status  : present
```

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 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 “Managing OmniSwitch 6350/6450 Series Stacks” chapter in the *Hardware Users Guide*.

Release History

Release 6.6.1; command introduced.

Related Commands

show stack topology	Displays the current operating topology of switches within a stack.

MIB Objects

```
alaStackMgrStackStatus
alaStackMgrTokensUsed
alaStackMgrTokensAvailable
```

show stack mode

Displays the current stacking or standalone mode of the switch.

show stack mode

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> show stack mode
NI      Role      State     Running        Saved
                            Mode           Mode
----+-----------+--------+----------+---------------
   1   PRIMARY    RUNNING  stackable     stackable
   2   SECONDARY  RUNNING  stackable     stackable
```

output definitions

NI	The current slot position for each switch in the virtual chassis (stacked configuration). 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 assign these slot numbers, use the **stack set slot** command.
Role	The current management role of the corresponding switch: 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].

output definitions (continued)

State	The current operational state of the switch: UNKNOWN: the state of the element cannot be determined RUNNING: element is up and running DUP SLOT: this element has a duplicate slot number CLR SLOT: the slot number of the element has been cleared using the management command after the last reboot OUT SLOT: the element cannot initialize because there are no slot IDs left to be assigned
Running Mode	The current mode of the switch.
Saved Mode	The mode of the switch after reboot. The output is based on contents of "boot.slot.cfg" file.

Release History

Release 6.6.1; command introduced.

Related Commands

stack set slot mode	Changes the stacking/standalone mode of the switch.

MIB Objects

```
alaStackMgrChassisTable
   alaStackMgrSlotNINumber
   alaStackMgrSlotCMMNumber
   alaStackMgrChasRole
   alaStackMgrChasState
   alaStackMgrCommandAction
   alaStackMgrCommandStatus
```

show hash-control

Displays the current hash control settings for the switch.

show hash-control [mode fdb]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show hash-control mode fdb
FDB Hash Mode = XOR-Mode

-> show hash-control
FDB Hash Mode = XOR-Mode,
FDB Hash Chain Length = DEFAULT,
Non-ucast Hash Status = Enable
```

output definitions

FDB Hash Mode	The current hash mode activated (XOR-Mode or CRC-Mode).
FDB Hash Chain Length	The configured value for the depth of the hashing bucket.
Non-ucast Hash Status	The hash control setting for non-unicast traffic (Enabled or Disabled).

Release History

Release 6.6.3; command introduced.
Release 6.7.2.R06; **Non-ucast Hash Status** field added.

Related Commands

hash-control mode fdb	Configures the hash control method on the switch. Depending on this configuration, hashing algorithm used by various applications for Layer 2 table lookup is affected.
hash-control load-balance non-ucast	Enable or disable the hashing for non-unicast traffic, which will load balance the non-unicast traffic across all ports in the linkagg at a global level.

MIB Objects

```
alaChasHashMode
alachasFdbHashMode
alachasNonUCHashControl
```

show system hardware-self-test

Displays the major hardware components status.

show system hardware-self-test

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

This command is applicable only in Authenticated Switch Access - Enhanced Mode. For more information on ASA mode commands, refer to the Chapter 49, "AAA Commands."

Examples

```
-> show system hardware-self-test
Checking CPU status -> Ok
Checking Memory status -> Ok
Checking Flash Status -> Ok
Checking NI Module status -> Ok
Checking Power Supply status -> Ok
Checking Lanpower Status -> Ok
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

show system process-self-test	Displays the major software process status.

MIB Objects

N/A

show system process-self-test

Displays the major software process status.

show system process-self-test

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

This command is applicable only in Authenticated Switch Access - Enhanced Mode. For more information on ASA mode commands, refer to the “AAA Commands” chapter of the *OmniSwitch AOS Release 6350/6450 CLI Reference Guide*.

Examples

```
-> show system process-self-test
Checking Chassis Supervision Process .....................OK
Checking Configuration Manager Process ....................OK
Checking Network Process ...................OK
Checking AAA Process ...................OK
Checking 802.1x Process ...................OK
Checking QoS Process ...................OK
Checking VLAN Manager Process ...................OK
Checking IP Services Process ...................OK
Checking H/W Driver Process ...................OK
Checking IPV6 Process ...................OK
Checking Layer2 / Switching Process ...................OK
Checking Layer3 / Routing Process ...................OK
Checking NiSUP Process ...................OK
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

show system hardware-self-test Displays the major hardware components status.

MIB Objects

N/A

license apply

Activates the license for licensed features on the switch.

license apply

Syntax Definitions

N/A

Defaults

By default, licensed features are not activated on the switch.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- 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 6.6.3; command introduced.

Related Commands

license remove	Removes the licensed applications installed on the switch.
show license file	Displays the license file information of the switch.
show license info	Displays all the license information for the switch.

MIB Objects

```
aluLicenseManagerApplyLicense
aluLicensedFileName
```

license remove

Removes the license for specified feature on the switch.

license remove feature {metro | gig | 10G}

Syntax Definitions

metro	Removes Metro features.
gig	Removes Gigabit interfaces on lite models.
10G	Removes 10-Gigabit interfaces.

Defaults

By default, licensed features are not activated on the switch.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use **show license file** command to verify the removed licenses.

Examples

```
-> license remove feature metro
```

Release History

Release 6.6.3; command introduced.

Related Commands

license apply	Applies the licensed applications installed on the switch.
show license file	Displays the license file information of the switch.
show license info	Displays all the license information for the switch.

MIB Objects

```
aluLicenseManagerRemoveTable
   aluLicenseRemoveFeatureID
   aluLicenseRemoveSlotID
```

license unlock

Temporarily activates the license feature on the switch.

license unlock feature {metro | gig | 10G}

Syntax Definitions

metro	Temporarily activates the metro license features.
gig	Temporarily activates the Gigabit interface license feature.
10G	Temporarily activates the 10-Gigabit license feature.

Defaults

By default, licensed protocols are not activated on the switch.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- When the **license unlock** 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 unlock feature metro
```

Release History

Release 6.6.3; command introduced.

Related Commands

show license file	Displays the license file information of the switch.
show license info	Displays all the license information for the switch.

MIB Objects

```
aluLicenseManagerDemoLicenseTable
   aluLicenseDemoFeatureID
   aluLicenseDemoSlotID
```

show license info

Displays all the licensed applications installed on the switch.

show license info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use this command to verify the licenses 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
(* indicates primary NI)

Chassis: METRO

NI         Application          License Type       Time Left (In Days)
-------+------------------+----------------------+-----------------
1(*)        METRO               Permanent               -
1 (*)       GIG                 Temporary              10
1002        GIG                 Temporary              5
3           METRO               Permanent              -
3           GIG                 Temporary              12
```

output definitions

Application	Displays the name of the licensed applications installed on the switch.
License Type	The type of license; Permanent or Temporary.
Time Left	Number of days remaining for temporary license.

Release History

Release 6.6.3; command introduced.

Related Commands

license apply	Applies the license file to the switch.
license remove	Removes the license from the switch.

MIB Objects

```
aluLicenseManagerInfoTable
   aluLicensedApplication
   aluLicenseType
   aluLicenseTimeRemaining
```

show license file

Displays the information contained in the license file.

show license file [*filename* | **local]**

Syntax Definitions

filename	The path and name of the license file.
local	Displays the file on the local switch only.

Defaults

parameter	default
filename	/flash/lmLicense.dat

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use this command to display the contents of the 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*     METRO
00:d0:95:d5:e6:0a      GIG
00:d0:95:d5:e6:0b      GIG
00:d0:95:d5:e6:0c*     METRO

* - 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 6.6.3; command introduced.

Related Commands

show license info	Displays all the licensed applications installed on the switch.

MIB Objects

```
aluLicenseManagerLicenseInfoTable
   aluSwitchMacAddress
   aluLicensedFileApplication
```

stack split-protection

Enables or disables the stack split detection feature.

stack split-protection {enable | disable}

Syntax Definitions

enable	Enables stack split protection.
disable	Disables stack split protection.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- SSP cannot be enabled before assigning a Linkagg.
- Stack split protection cannot be enabled on a device that is already running the helper functionality.
- In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> stack split-protection enable
-> stack split-protection disable
```

Release History

Release 6.6.5; command was introduced.

Related Commands

show stack split-protection status	This command displays all the information related to SSP when enabled.
stack split-protection linkaggid	This command is used to assign a linkagg for use with SSP.

MIB Objects

```
AlcatelIND1StackManager
   alaSspConfigStatus
```

stack split-protection linkaggid

This command is used to assign a linkagg for use with SSP.

[no] stack split-protection linkaggid *linkagg-id*

Syntax Definitions

linkagg-id	The link aggregate ID to be used with SSP. The range is 0-128.

Defaults

parameter	default
N/A	

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command must be used to configure stack split protection linkagg before enabling stack split protection.
- In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> stack split-protection linkaggid 1
```

Release History

Release 6.6.5; command was introduced.

Related Commands

show stack split-protection status	This command displays all the information related to SSP when enabled.
show stack split-protection statistics	This command shows statistics of stack split-protection.

MIB Objects

```
AlcatelIND1StackManager
   alaSspLinkaggID
```

stack split-protection guard-timer

This command sets the timer value for how long the unit will wait to receive SSP PDUs before beginning transmission of SSP PDUs.

stack split-protection guard-timer *time*

Syntax Definitions

time	Time interval to wait on boot up before choosing any state. Range is 30-100 seconds.

Defaults

parameter	default
time	30 seconds

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Changes to the Guard timer only take affect after reboot or by disabling and re-enabling stack split protection.
- In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> stack split-protection guard-timer 60
```

Release History

Release 6.6.5; command was introduced.

Related Commands

show stack split-protection status	This command displays all the information related to SSP when enabled.
show stack split-protection statistics	This command shows statistics of stack split-protection.

MIB Objects

```
AlcatelIND1StackManager
   alaSspGuardTimer
```

stack split-protection helper

This command is used to enable or disable to helper functionality on the helper device.

stack split-protection helper {enable | disable}

Syntax Definitions

enable	Enables stack split protection helper functionality.
disable	Disables stack split protection helper functionality.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command on the helper device to enable the helper functionality.
- The helper functionality cannot be enabled on a device that is running stack split protection.
- In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> stack split-detection helper enable
-> stack split-detection helper disable
```

Release History

Release 6.6.5; command was introduced.

Related Commands

stack split-protection helper linkagg	Linkagg ID on which to apply the SSP protocol for the helper device.

MIB Objects

```
AlcatelIND1StackManager
   alaSspHelperConfigStatus
```

stack split-protection helper linkagg

Linkagg ID on which to apply the SSP protocol on the helper device.

stack split-detection helper linkagg *linkagg-id*

Syntax Definitions

linkagg-id	Linkagg ID associated to the helper to support SSP. Range is 0-31.

Defaults

parameter	default
N/A	

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command on the helper device to enable the SSP protocol on the helper linkagg.
- In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> stack split-protection helper linkagg 1
```

Release History

Release 6.6.5; command was introduced.

Related Commands

show stack split-protection helper status	This command shows SSP Helper status of the Link Aggregation ID assigned.
stack split-protection helper	This command is used to enable or disable to helper functionality.

MIB Objects

```
AlcatelIND1StackManager
   alaSspHelperLinkaggId
```

show stack split-protection status

This command displays all the information related to SSP when enabled.

show stack split-protection status

Syntax Definitions

N/A

Defaults

parameter	default
N/A	

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> show stack split-protection status
SSP admin status:       enabled
SSP operational status: Active
SSP linkagg:            31
SSP Guard Timer:        30
```

Release History

Release 6.6.5; command was introduced.

Related Commands

stack split-protection	Enable or disables the stack split detection feature.

MIB Objects

```
AlcatelIND1StackManager
   alaSspConfigStatus
   alaSSpGuardTimer
```

show stack split-protection statistics

This command shows statistics of stack split-protection.

show stack split-protection statistics

Syntax Definitions

N/A

Defaults

parameter	default
N/A	

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> show stack split-protection statistics
SSP admin status:       Enable
SSP operational status: Active
SSP uptime:             10d:02h:15m:31s
SSP protection uptime:  00d:00h:00m:00s
```

Release History

Release 6.6.5; command was introduced.

Related Commands

stack split-protection	Enable or disables the stack split detection feature..

MIB Objects

```
AlcatelIND1StackManager
   alaSspConfigStatus
   alaSspUptime
   alsSspStateUptime
```

show stack split-protection stacking-units

This command shows the SSP state of all stacked units.

show stack split-protection stacking-units

Syntax Definitions

N/A

Defaults

parameter	default
N/A	

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> show stack split-protection stacking-units

Stacking Units - SSP States
---------------------------
SLOT    STATE
----------------------
 1      ACTIVE
 2      ACTIVE
```

Release History

Release 6.6.5; command was introduced.

Related Commands

stack split-protection	Enable or disables the stack split detection feature.

MIB Objects

```
AlcatelIND1StackManager
   alaStackMgrSlotNINumber
   alaSSpOpStatus
```

show stack split-protection helper status

This command shows SSP Helper status of the Link Aggregation ID assigned.

show stack split-protection helper status

Syntax Definitions

N/A

Defaults

parameter	default
N/A	

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

In OmniSwitch 6350, stacking is only supported on the 24 or 48 port models.

Examples

```
-> show stack split-protection helper status
Stack Split-Protection Helper Status : Disabled
 Link Aggregation Id            Stack Split-Protection Status
------------------------+-----------------------------------------------------
           3                        Disabled
```

Release History

Release 6.6.5; command was introduced.

Related Commands

stack split-protection helper This command is used to enable or disable the helper functionality.

MIB Objects

```
AlcatelIND1StackManager
   alaSspHelperAggregateId
   alaSspHelperAggregateStatus
```

3 Chassis MAC Server (CMS) Commands

The Chassis MAC Server (CMS) manages MAC addresses on the switch. The MAC addresses managed through 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.

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 6450, 6350

Usage Guidelines

- Because the factory-installed 32 MAC addresses are sufficient for most network configurations, this command has to be used only 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 is not be allocated properly.
- All MAC addresses in a range must be contiguous (that is, 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

If the old primary switch is not detected and included in the stack within a pre-defined time period, an SNMP trap is generated.

Examples

```
-> mac-retention dup-mac-trap enable
```

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

The MAC address is released only if the address has not been derived from the EEPROM (that is, it has to be a retained MAC address of the old primary switch).

Examples

```
-> mac release
```

Release History

Release 6.6.1; command was introduced.
Release 6.6.1; **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 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

If you are assigning VLAN router ports while the switch is in *single MAC router mode*, all VLAN router ports uses 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 3-7 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 6.6.1; 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 6450, 6350

Usage Guidelines

- If the administrative status of MAC retention is not configured, it is displayed as disabled by default.
- If the administrative status of the duplicate MAC address trap is not configured, it is displayed as disabled by default.
- If the source of the currently used MAC address is not configured, it is 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 6.6.1; command was introduced.
Release 6.6.1; **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
```

4 Power over Ethernet (PoE) Commands

The Power over Ethernet (PoE) feature is supported on the OmniSwitch PoE models. See the *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 through Ethernet ports. For consistency, this chapter and the *OmniSwitch AOS Release 6 CLI Reference Guide* see 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, and so on.
- *PSE* refers to the actual hardware source of the electrical current for PoE.

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

MIB information for the PoE commands is as follows:

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

Filename: AaIETF_HUBMIB_POWER_ETHERNET_DRAFT_mib
Module: POWER-ETHERNET-MIB

A summary of the available commands is listed here:

lanpower start
lanpower delayed-start
lanpower stop
lanpower power
lanpower maxpower
lanpower priority
lanpower priority-disconnect
lanpower combo-port
lanpower high-resistance-detection
lanpower capacitor-detection
show lanpower
show lanpower delayed-start
show lanpower capacitor-detection
show lanpower priority-disconnect
show lanpower high-resistance-detection

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 through the **lanpower stop** command.
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).
slot	Activates inline power on all PoE ports in the corresponding slot.

Defaults

Power over Ethernet operational status is globally enabled by default.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.
Release 6.7.2.R01; default setting was changed to enabled.

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 delayed-start

Allows to set a timer to delay the startup of Power over Ethernet (PoE) ports in a specified slot when the switch is powered up or rebooted.

lanpower *slot* **delayed-start {enable | disable} [***value***]**

Syntax Definitions

slot	The slot ID in which the delayed start for PoE port must be enabled or disabled.
enable | disable	Enable or disable the delayed start for PoE port.
value	The delay timer in seconds. The delay timer must be between 120 and 600 seconds.

Defaults

The delayed start operational status is globally disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The slot ID must be specified to activate the delayed start of the PoE ports on that slot.
- The delayed timer is applied only during bootup and not when the LAN power is manually restarted. The LAN power is started after the delay timer expiry.
- The LAN power cannot be started or stopped if the delay timer is activated on the slot.

Examples

```
-> lanpower 5 delayed-start enable 200
-> lanpower 5 delayed-start disable
```

Release History

Release 6.7.2.R04; command was introduced.

Related Commands

show lanpower delayed-start	Displays if the delayed timer is set for PoE ports in a specified slot.

MIB Objects

```
alaPethMainPseGroup
   alaPethMainPseDelayStartStatus
   alaPethMainPseDelayStartValue
```

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 (for example, 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 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; 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.
lanpower combo-port	Displays current inline power status and related statistics for all PoE ports in a specified slot.

MIB Objects

```
alaPethMainPseGroup
   alaPethMainPseAdminStatus
pethPsePortTable
   pethPsePortAdminEnable
```

lanpower power

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

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

Syntax Definitions

slot/port	A PoE port on which the maximum amount of inline power is being allocated.
milliwatts	The maximum amount of inline power, in milliwatts, being allocated to the corresponding port (3000–16000 or 3000-31000).

Defaults

parameter	default
milliwatts (802.3af ports)	16000
milliwatts (802.3at ports)	31000

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- To globally specify the amount of inline power allocated to *all ports in a slot*, see the **lanpower maxpower** command on page 4-7.
- 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 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
alaPethPsePortTable
   alaPethPsePortPowerMaximum
```

lanpower maxpower

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

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

Syntax Definitions

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

Defaults

parameter	default
watts	Will vary based on model and power supply.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Before changing the maximum slot-wide power allowance, you have to disable PoE for the slot through the **lanpower stop** command. Once the new value is assigned, re-enable PoE for the slot through the **lanpower start** command.
- To specify the maximum amount of inline power allocated to a *single port*, see the **lanpower power** command on page 4-5.
- 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 6.6.1; command was introduced.

Related Commands

lanpower power	Specifies the maximum amount of inline power, in milli-watts, allocated to a specific PoE port.
lanpower combo-port	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 (that is, 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 (that is, before critical- and high-priority ports).

Defaults

parameter	default
low | high | critical	low

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; command was introduced.

Related Commands

lanpower combo-port	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 is 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, see the "Managing Power over Ethernet (PoE)" chapter in the *OmniSwitch AOS Release 6.7 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 is granted or denied power. For information on priority disconnect rules, see the "Managing Power over Ethernet (PoE)" chapter in the *OmniSwitch AOS 6.7 Series*.
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 is denied to *any* incoming PD, regardless of its priority status.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; 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 combo-port

Enables or disables PoE capability on the copper combo ports.

lanpower *slot* **combo-port {enable | disable}**

Syntax Definitions

slot	The particular slot on which to enable or disable PoE capability on the copper combo ports.
enable	Enables PoE capability on the copper combo ports 25/26 and disables PoE capability on ports 23/24.
disable	Disables PoE capability on the copper combo ports 25/26 and enables PoE capability on ports 23/24.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

N/A

Usage Guidelines

Port pairs 23/24 and 25/26 cannot have PoE enabled at the same time. Use this command to choose which port pairs support PoE.

Examples

```
-> lanpower 1 combo-port enable
```

Release History

Release 6.6.1; 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

N/A

lanpower high-resistance-detection

Enables or disables two-port PoE PD detection.

lanpower *slot* **high-resistance-detection {enable | disable}**

Syntax Definitions

slot	The particular slot on which to enable or disable high-resistance-detection.
enable	Enables high-resistance-detection capability on the slot.
disable	Disables high-resistance-detection capability on the slot.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This capability can be enabled to support the two-port PoE capability on APs with two PoE ports (i.e. OAW-AP 130 Series or OAW-AP1251). This capability enables the switch to support the appropriate detection range and recognize the AP as a PD.
- The AP will be powered in an active/standby mode, meaning only one port of the AP will be powered at a time.
- Only two-pair PoE will be supported when this feature is enabled, even on ports connected with a 4-pair Ethernet cable.
- The capability of PSE-to-PSE protection function is reduced when this feature is enabled. It is recommended to disable PoE on ports that do not have PDs connected.
- Enabling this feature will cause the PoE functionality to restart on the OmniSwitch. Additionally, this functionality does not follow the PoE IEEE standards.

Examples

```
-> lanpower 1 high-resistance-detection enable
```

Release History

Release 6.7.2.R03; command was introduced.

Related Commands

show lanpower high-resistance-detection Displays current high-resistance-detection settings.

MIB Objects

```
alaPethMainPseTable
   alaPethMainPseHighResistorDetect
```

lanpower capacitor-detection

Enables or disables the capacitor detection method.

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

Syntax Definitions

slot	The particular slot on which to enable capacitor-detection.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6450, 6350

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 Enterprise sales engineer or Customer Support representative to find out which Alcatel-Lucent Enterprise IP phones models need capacitive detection enabled.
- Enabling capacitor-detection will cause lanpower to be restarted.
- A non-PD device may also receive lanpower if capacitor is detected.

Examples

```
-> lanpower 1 capacitor-detection enable
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show lanpower capacitor-detection	Displays the capacitor detection method status.

MIB Objects

```
alaPethMainPseTable
   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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show lanpower 1
Port Maximum(mW) Actual Used(mW)   Status    Priority  On/Off   Class
----+-----------+---------------+-----------+---------+------+-------
  1     31000            0       Undefined      Low      OFF      -
  2     31000            0       Undefined      Low      OFF      -
  3     31000            0       Undefined      Low      OFF      -
  4     31000            0       Undefined      Low      OFF      -
  5     31000            0       Undefined      Low      OFF      -
  6     31000            0       Undefined      Low      OFF      -
  7     16000            0       Undefined      Low      OFF      -
(Output truncated)
 22     16000            0       Undefined      Low      OFF      -
 23     31000            0       Undefined      Low      OFF      -
 24     31000            0       Undefined      Low      OFF      -

Slot 1 Max Watts 225
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 allocated to the corresponding PoE port, in milliwatts. The default value is 15400. To change this setting, use the **lanpower power** command.
Actual Used (mW)	The actual amount of power being used by an attached device (if applicable), in milliwatts. If no device is attached to the corresponding port, this row displays a value of 0.

output definitions (continued)

Status	**Powered Off** - Port is off. User command set port to off. **Powered On** - Port is on. Valid resistor / 802.3af-compliant Powered Device (PD) or valid capacitor / 802.3at-compliant PD was detected or 802.3af/at-compliant PD is powered on 4-pair lines or higher PD is connected. **Undefined** - The device returned an unknown port status for the software. **Searching** - Interim state during line detection or non-standard PD detected. Status will change after detection process is completed. (Deny Status Descriptions - Power Manager Algorithms have denied power to this channel either due to priority disconnect or over subscription.) **Denied VHI** - Port is off. Volts higher than maximum volt. **Denied VLO** - Port is off. Volts lower than minimum volt. **Denied UDL** - Port is off. Underload state according to 802.3af (current is below Imin). **Denied OVL** - Port is off. Overload state according to 802.3af (current is above Icut). **Denied PM** - Port is off. Power management function shut down port due to lack of power. Port is shut down or remains off. **Denied PM** - Port is off. Static power management - calculated power > power limit. **Denied PM** - Port is off. Static power management and overload - PD class report > user predefined power value. **Class Error** - Port is off. Illegal class error. **Bad!VoltInj** - Port is off. Port fails due to voltage being applied to the port from external source. (Fault Status Descriptions- Activation or class detection has failed, or an active channel has violated a boundary parameter.) **Faulty Port** - Port is off. Hardware pin disables all ports or fewer ports are available than the maximum number of ports that the controller can support. Unavailable ports are considered 'off'. **Fault S/W**- Port is off. This status indicates a software problem. **Fault UD/OV** - Port is off. Succession of underload and overload states caused port shutdown. May be also caused by a PD's DC/DC fault. **Fault H/W** - Port is off. Hardware problems preventing port operation or port does not respond to hardware fault or system initialization. **Fault CAPDE** - Port is off. Failure due to out-of-range capacitor value. **Fault DISCH** - Port is off. Port failure due to system voltage supply through other port. Check other port for status 0x24. This error is linked with mask 0x1F enable. **Fault Short** - Port is off. Short condition was detected. **Fault Temp** - Port is off. Port temperature protection mechanism was activated. **Fault HiTEM** - Port is off. Die temperature is above safe operating value. **Faulty Chip** - Port is off. Sum of square currents exceeded.

output definitions (continued)

Priority	The current priority level for the corresponding PoE port. Options include **Critical**, **High**, and **Low**. **Critical** has to be reserved for ports that have mission-critical devices attached, and therefore require top (that is, 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 (that is, before critical and high-priority ports). The default value is Low. Priority levels is 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 through the **lanpower start** command. **OFF** indicates that the port has been turned off by the user through the **lanpower stop** command.
Max Watts	The maximum watts allocated to the corresponding slot. The maximum watts value for a slot is changed using the **lanpower maxpower** command.
Class	Displays the IEEE class of the PoE based on the power consumption.

Release History

Release 6.6.1; command was introduced.

Related Commands

N/A

MIB Objects

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

show lanpower delayed-start

Displays if the delayed timer is set for PoE ports in a specified slot.

show lanpower delayed-start *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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show lanpower delayed-start 1
Delay Start Status enable
Delay Start Value 200
```

output definitions

Delay Start Status	Displays the operational status of delayed timer.
Delay Start Value	Displays the timer value set for delayed start of PoE ports.

Release History

Release 6.7.2.R04; command was introduced.

Related Commands

lanpower delayed-start	Allows to set a timer to delay the startup of Power over Ethernet (PoE) ports in a specified slot.

MIB Objects

```
alaPethMainPseGroup
   alaPethMainPseDelayStartStatus
   alaPethMainPseDelayStartValue
```

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 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; 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 high-resistance-detection

Displays the current high-resistance-detection settings.

show lanpower high-resistance-detection *slot*

Syntax Definitions

slot	The particular slot on which to display the high-resistance-detection settings.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show lanpower high-resistance detection 1
High Resistance Detection enabled on Slot 1
```

Release History

Release 6.7.2.R03; command was introduced.

Related Commands

llanpower high-resistance-detection	Enables or disables two-port PoE PD detection.

MIB Objects

N/A

5 Network Time Protocol Commands

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

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

The MIB information for NTP is as follows:

Filename: AlcatelIND1Ntp.mib
Module: alcatelIND1NTPMIB

A summary of available commands is listed here:

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

ntp server

Specifies an NTP server from which the switch receives updates.

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

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

Syntax Definitions

ip_address	The IP address of the NTP server to be added or deleted to the client's server list.
domain_name	The domain name of the NTP server to be added or deleted to the client's server list. This is usually a text string.
key	The key identification number that corresponds to the specified NTP server.
version	The version of NTP being used. This is 1, 2, 3, or 4.
exponent	The number of seconds between polls to this server. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds ($2^4 = 16$).
prefer	Marks this server as the preferred server. A preferred server's timestamp is used before another server.
burst	Enables burst mode. The burst mode allows the exchange of eight NTP messages (instead of one) when the server is reachable and at each poll interval to achieve faster synchronization. The spacing between the first and the second packet is 16 seconds to allow a modem call to complete, while the spacing between the remaining packets is 2 seconds.
iburst	Enables initial burst (iburst) mode. The iburst mode allows immediate exchange of eight NTP messages (instead of one) when the server is unreachable and at each poll interval, to achieve faster initial synchronization acquisition. The spacing between the packets is 16 seconds to allow a modem call to complete. Once the server is reachable, the spacing between the packets is 2 seconds.

Defaults

Parameter	Default
version	4
exponent	6
prefer	not preferred
burst	no burst
iburst	no iburst

For NTP pool servers, iburst is configured as the default mode.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to delete the specified server.
- To configure NTP in the client mode you have to first define the NTP servers.
- 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 has to 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 polls the server for a time update when the **minpoll** time is exceeded.
- Burst mode of operation improves timekeeping quality with the server command and iburst mode of operation is designed to speed the initial synchronization acquisition with the server command.

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
-> ntp server 1.1.1.1 burst
-> ntp server 1.1.1.1 iburst
-> no ntp server 1.1.1.1
```

Release History

Release 6.6.1; command was introduced.
Release 6.7.2.R05: **burst** and **iburst** keywords added.

Related Commands

ntp client	Enables or disables NTP operation on the switch.
show ntp client server-list	Displays a list of the servers with which the NTP client synchronizes.
show ntp server status	Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

```
alaNtpConfig
   alaNtpPeerAddressType
   alaNtpPeerType
   alaNtpPeerAuth
   alaNtpPeerVersion
   alaNtpPeerMinpoll
   alaNtpPeerPrefer
   alaNtpPeerAddress
   alaNtpPeerBurst
   alaNtpPeerIburst
```

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 6450, 6350

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 6.6.1; 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 6450, 6350

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 finally synchronizes with an atomic clock.

Examples

```
-> ntp server unsynchronized
```

Release History

Release 6.6.1; 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 operation on the switch.

ntp client {enable | disable}

Syntax Definitions

enable	Enables NTP.
disable	Disables NTP.

Defaults

NTP protocol is disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

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

Release History

Release 6.6.1; command was introduced.

Related Commands

ntp server	Specifies an NTP server from which the switch receives updates.

MIB Objects

```
alaNtpEnable
```

ntp broadcast

Enables or disables the client's broadcast mode.

ntp broadcast {enable | disable}

Syntax Definitions

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

Defaults

Broadcast mode is disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

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

Release History

Release 6.6.1; 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.

ntp broadcast delay *microseconds*

Syntax Definitions

microseconds	The number of microseconds for the broadcast delay.

Defaults

parameter	default
microseconds	4000

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

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

Release History

Release 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
alaNtpBroadcastDelay
```

ntp key

Labels the specified authentication key identification as trusted or untrusted.

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

Syntax Definitions

key	The key number matching an NTP server.
trusted	Signifies 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 does not occur with an untrusted authentication key.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

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

Release History

Release 6.6.1; 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 authentication on the switch.

MIB Objects

```
alaNtpAccessKeyIdTable
   alaNtpAccessKeyIdKeyId
   alaNtpAccessKeyIdTrust
```

ntp key load

Loads the current key file into memory.

ntp key load

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 has to be labeled as **trusted** with the **ntp key** command before being used for authentication.

Examples

```
-> ntp key load
```

Release History

Release 6.6.1; 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 receives updates.

MIB Objects

```
alaNtpAccessRereadkeyFile
```

show ntp client

Displays information about the current client NTP configuration.

show ntp client

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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:                   Fri, May 4 2018  9:46:31.467 (UTC),
Last NTP update:                Fri, May 4 2018  9:45:45.567 (UTC),
Server reference:               clock1.ovcirrus.com [52.66.5.185],
Client mode:                    enabled,
Broadcast client mode:          disabled,
Broadcast delay (microseconds): 4000,
Server qualification:           unsynchronized
```

output definitions

Current time	The current time for the NTP client.
Last NTP update	The time of the last synchronization with an NTP server.
Server reference	Displays the NTP pool servers in IP address as well as FQDN format according to the format in which the particular server was configured.
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	Specifies server qualification, synchronized or unsyncronized.

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ntp client server-list
IP Address                          Ver Key  St  t  When   Poll   Reach   Delay   Offset  Disp
------------------------------------+---+---+----+--+-----+------+-------+-------+--------+-----
*clock2.ovcirrus.com[139.59.82.60]    4   0   2   u    1    1024     f     0.117   -0.042  0.078
=clock3.ovcirrus.com[123.108.200.124] 4   0   3   u   55    1024     2     0.083   -0.025  0.016
```

output definitions

IP Address	Displays NTP servers in IP address as well as FQDN format according to the format in which the particular server was configured.
Ver	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This has to be accurate and the same as the NTP server, or the client switch is unable to synchronize with the NTP server. A zero (0) means there is no key entered.
St	The stratum of the server.
t	Type of server (l - local, u - unicast, m - multicast, b - broadcast)
When	Number of seconds passed since last response from remote host.
Poll	Polling interval to the remote host in seconds.
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 6.6.1; command was introduced.
Release 6.7.2.R05; t, poll, and when fields added.

Related Command

ntp client	Enables or disables authentication on the switch.

MIB Objects

```
alaNtpPeerListTable
```

show ntp server status

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

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

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show ntp server status
IP address         = clock3.ovcirrus.com [123.108.200.124],
Host mode          = client,
Peer mode          = server,
Prefer             = no,
Version            = 4,
Key                = 0,
Stratum            = 2,
Minpoll            = 6 (64 seconds),
Maxpoll            = 10 (1024 seconds),
Poll               = 1024,
when               = 283,
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 NTP server in IP address as well as FQDN format according to the format in which the particular server was configured.
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 has to be accurate and the same as the NTP server, or the client switch is 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 polls the server for a time update every time this limit has been exceeded.
Maxpoll	The maximum poll time.
Poll	Number of seconds passed since last response from remote host.
When	Polling interval to the remote host in seconds.
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.

output definitions (continued)

Bad dispersion	Number of bad dispersions.
Last Event	The last event.

Release History

Release 6.6.1; command was introduced.
Release 6.7.2.R05; poll and when fields added.

Related Command

ntp client	Enables or disables authentication 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 6450, 6350

Usage Guidelines

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

Examples

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

output definitions

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

Release History

Release 6.6.1; 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
```

6 Session Management Commands

Session Management commands are used to monitor and configure operator sessions including FTP, Telnet, HTTP (WebView), console, Secure Shell, and Secure Shell FTP on the switch. (See the SNMP Commands chapter for SNMP session commands.)

Maximum number of concurrent sessions allowed are:

Session	OmniSwitch 6350/6450
Telnet (v4 or v6)	6
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 console
session xon-xoff
session cli-auto-complete-space
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
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 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

Session login-timeout is not applicable for SSH, since SSH timeout is based on the calculation as per the openSSH code.

Examples

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

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; command introduced.

Related Commands

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

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 6450, 6350

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 6.6.1; command introduced.

Related Commands

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

MIB Objects

```
SessionConfigTable
   SessionType
   SessionInactivityTimerValue
```

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 6350”**
system-name	Sets the prompt to the current system name of the switch. By default, the system name is set to ‘VxTarget’.

Defaults

parameter	default
string	->
system-name	VxTarget

Platforms Supported

OmniSwitch 6450, 6350

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 2-4 in Chassis Management and Monitoring Commands chapter.
- Every time the system name is modified, the prompt also gets modified.
- In case the system name is larger than 35 characters, prompt is truncated to 35 characters.
- The new prompt takes effect after relogging to a new session.

Examples

```
-> session prompt default
-> session prompt default system-name
```

Release History

Release 6.6.1; command introduced.
Release 6.6.3; 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 console

Enable or disable switch access through the console port of the switch.

session console {enable | disable}

Syntax Definitions

enable	Enables the switch access through the console port through the CLI shell.
disable	Disables the switch access through the console port through the CLI shell.

Defaults

parameter	default
enable | **disable**	enable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- It is recommended to create a back-up of the configuration file before using this command. contact customer support to recover the switch.
- Before disabling the CLI console shell, configuration for telnet access with proper user privilege must be made.
- The command must be issued only through telnet or SSH session, and not through console sessions.
- When the CLI console shell is disabled, the switch log output to the console is also disabled.
- When the CLI console shell is disabled, switch can be accessed through SSH or telnet or WebView session.
- The command can be stored to the configuration file using write memory.
- If this command is disabled and the telnet or SSH or WebView access to the switch is also lost, set the bootflags to 0x1000 and stop the switch in miniboot. Once the switch stops in miniboot, delete the configuration file and reboot the switch to get console access to the switch. Alternatively, contact customer support.

Note. Deleting configuration file will also delete the other configurations. Hence, it is recommended to create a back-up of the configuration file before deleting the configuration file.

Examples

```
-> session console disable
-> session console enable
```

Release History

Release 6.6.5; 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
   sessionConsoleStatus
```

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 6450, 6350

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 6.6.1; command introduced.

Related Commands

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

MIB Objects

```
sessionXonXoffEnable
```

session cli-auto-complete-space

Enables/disables the CLI auto completion using space key.

session cli-auto-complete-space {enable | disable}

Syntax Definitions

enable	Enables CLI auto completion on the switch.
disable	Disables CLI auto completion on the switch.

Defaults

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

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Auto completion of CLI command can be enabled or disabled using this command.
- With CLI auto-complete feature enabled, the space key can be used for auto completion of the CLI command similar to the TAB key. If an incorrect keyword is entered, pressing the TAB key will remove the keyword.

Examples

```
-> session cli-auto-complete-space enable
-> session cli-auto-complete-space disable
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

show session config	Displays session manager configuration information (for example, default prompt, banner file name, inactivity timer, login timer, login attempts, and CLI console shell status).

MIB Objects

```
sessionCliAutoCompleteSpace
```

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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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*

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.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- 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
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 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 6450, 6350

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 6.6.3; 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> user profile reset
```

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> history size 10
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6-33 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 6-33 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 6-33 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 6-33 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 6.6.1; 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 6450, 6350

Usage Guidelines

- You can identify your current login session by using IP address.
- This command applies to the following session types: Console, Telnet, SSH, FTP, SFTP, HTTP, HTTPS, SNMP.

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.
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 6-35 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 6-35 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 6-35 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 6-35 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 6.6.1; 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, login attempts, and CLI console shell status).

show session config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show session config

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

output definitions

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

output definitions (continued)

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.

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 space bar 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 {tcp-port *port-number* **|** *host_name* **|** *ip_address* | **enable** | **disable}**

Syntax Definitions

port-number	Specifies the TCP port number to be used for SSH. The TCP port numbers that can be configured for SSH port are either default port 22 or port numbers in the range 2048 - 65535.
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 6450, 6350

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.
- You can establish eight SSH sessions towards an OmniSwitch when it acts as Server. A maximum of three SSH sessions are allowed in a minute (utilities such as keyscan is also considered as a valid session). More than three sessions in a minute result in an SSH attack. A minute after an attack, only one SSH session per minute is allowed. If there is no SSH session created for the next three minutes after an attack, a maximum of three SSH sessions are allowed for a minute again.
- The configured TCP port number will be saved in the switch file **/flash/network/sshConfig.cfg**. The switch must be rebooted after configuring the TCP port number.
- Well-known reserved TCP port numbers (1-1024) and the IP ports which are internally used cannot be configured for the SSH TCP port.

Examples

```
-> ssh enable
-> ssh tcp-port 2048
-> ssh 172.155.11.211
login as:
```

Release History

Release 6.6.1; command introduced.
Release 6.7.1 R02; **tcp-port** parameter 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 6450, 6350

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 6.6.1; 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
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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6-29.

show command-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 AOS Release 6 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 6.6.1; 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.

show command-log status

Syntax Definitions

N/A

Defaults

Command logging is disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

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 6-29.

Release History

Release 6.6.1; 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
```

7 File Management Commands

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

MIB information for the system commands is as follows:

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

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

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's current working directory.

cd [*path***]**

Syntax Definitions

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

Defaults

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

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesWorkingDirectory
```

pwd

Displays the switch's current working directory.

pwd

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> pwd
/flash
```

Release History

Release 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesWorkingDirectory
```

mkdir

Creates a new directory.

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

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

rmdir

Deletes an existing directory.

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

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

ls

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

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

Syntax Definitions

-r	Optional syntax that displays the contents of the current directory in addition to *recursively* displaying all subdirectories. Be sure to include a space between the syntax **ls** and **-r** (that is, **ls -r**).
path/	Specifies the path (that is, 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

dir

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

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

Syntax Definitions

path/	Specifies the path (that is, 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesArg22
   systemServicesAction
```

rename

Renames an existing file or directory.

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

Syntax Definitions

path/	Specifies the particular path (that is, 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 6450, 6350

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 6.6.1; 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** (that is, **rm -r**).
path	The path (that is, 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 (for example, **test_config_file**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 has to 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 6.6.1; 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 (that is, 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 (for example, **test_config_file**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 has to 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 6.6.1; 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 sub-directories and files. Be sure to include a space between the syntax **cp** and **-r** (that is, **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 is 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 has to be different from the original. Up to thirty-two (32) characters may be used.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You have to verify that your switch's **/flash** directory has enough available memory to hold the new files and directories that results 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 6.6.1; 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 is 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 6450, 6350

Usage Guidelines

- This command prompts you to enter the admin password, and the names and the path of the files being copied is 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.
- SCP is not supported between OmniSwitch and Windows currently.

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 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesArg2
   systemServicesAction
```

mv

Moves an existing file or directory to a new location.

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

Syntax Definitions

path/	Specifies the path (that is, 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 (that is, 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 is 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 is used.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

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

Release History

Release 6.6.1; 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 (that is, 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 (that is, 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 is 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 is used.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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—that is, 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 6450, 6350

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 6.6.1; 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—that is, 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 6450, 6350

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 6.6.1; 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 6450, 6350

Examples

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

-> freespace
/flash 3143680 bytes free
```

Release History

Release 6.6.1; 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 is 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 6450, 6350

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 displays 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 6.6.1; command was introduced.

Related Commands

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

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

newfs

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

newfs /flash

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> newfs /flash
```

Release History

Release 6.6.1; command was introduced.

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 [*slot***:]** *source_filepath* **[***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.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

On switches in a stack configuration, this command copies a file from any non-primary switch to the primary switch in a stack. You have to 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
```

Release History

Release 6.6.1; 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 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 6450, 6350

Usage Guidelines

On switches in a stacked configuration, this command deletes a file from any non-primary switch. You have to specify the slot number on these switches.

Examples

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

Release History

Release 6.6.1; command was introduced.

Related Commands

rcp	Copies a file 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 switch in a stack.

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

Syntax Definitions

slot	The slot number of the non-primary switch in a stack.
directory	The name of the directory on the non-primary switch.
file_name	The file to be displayed on the non-primary switch.

Defaults

By default, all files in the specified directory are displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

This command displays directory content on any non-primary switch in a stack. You have to specify the slot number on these switches.

Examples

```
-> 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 6.6.1; 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's UNIX-like Vi text editor. The Vi file editor allows you to view or edit the contents of a specified text file.

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

Syntax Definitions

path	The path (that is, 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 (for example, **test_config_file**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> vi test_config_file
```

Release History

Release 6.6.1; 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 (for example, **test_config_file**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

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

Release History

Release 6.6.1; command was introduced.

Related Commands

vi	Launches the switch's Vi text editor.

MIB Objects

```
systemServices
   systemServicesArg1
   systemServicesAction
```

tty

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

tty *lines columns*

Syntax Definitions

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

Defaults

parameter	default
lines	24
columns	80

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 wraps to the next line displayed.
- If the text file contains more lines than set with the **tty** command, the switch displays only the number of lines specified. To display more lines, press the space bar 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 6.6.1; 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 6450, 6350

Usage Guidelines

- You have to 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 6.6.1; 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 6450, 6350

Usage Guidelines

- You need to 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's link-local address, the source interface name has to 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 6.6.1; 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> scp-sftp enable
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

- You need to 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 6.6.1; 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

```
SystemServices
   systemServicesArg1
   systemServicesAction
```

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 6450, 6350

Usage Guidelines

- You need to 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's link-local address, the source interface name has to 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

- To use Zmodem, you need to 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, use the **ls** command to verify that the files were loaded successfully.
- To abort a Zmodem session, enter **CTRL** + **X** five times in succession. Refer to your switch's User Manual for more information on uploading files via Zmodem.
- This command can also be used on the secondary CMM.

Examples

```
-> rz
Upload directory: /flash
rz ready to receive file, please start upload (or send 5 CTRL-X's to abort).
```

Release History

Release 6.6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
systemServices
   systemServicesAction
```

8 Web Management Commands

The switch can be configured and monitored using WebView, which is a web-based device management tool. Web Management CLI commands allow you to enable/disable web-based management and configure certain WebView parameters, such as Secure Socket Layer (SSL).

MIB information for the Web Management commands is as follows:

Filename: AlcatelInd1WebMgt.mib
Module: alcatelIND1WebMgtMIB

A summary of the available commands is listed here:

http server
http ssl
http port
https port
debug http sessiondb
show http
webview wlan cluster-virtual-ip
webview wlan cluster-virtual-ip precedence
show webview wlan config

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 6450, 6350

Usage Guidelines

Use the **no** form of this command to disable web management. If web management is disabled, you may be unable to access the switch using WebView.

Examples

```
-> http server
-> no http server
-> https server
-> no https server
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 has to be in the range 0 to 65535; well-known port numbers cannot be configured.

Defaults

parameter	default
port	80

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

All WebView sessions has to be terminated before entering this command.

Examples

```
-> http port 1025
-> http port default
```

Release History

Release 6.6.1; 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 has to be in the range 0 to 65535; well-known port numbers cannot be configured.

Defaults

parameter	default
port	443

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

All WebView sessions has to be terminated before entering this command.

Examples

```
-> https port 1026
-> https port default
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 is 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 6.6.1; 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
```

webview wlan cluster-virtual-ip

Configures the cluster virtual IP address of the Access Point (AP) in the switch. The WebView server on the switch redirects the URL to the AP (Virtual IP Address) URL when the WLAN Management is accessed from WebView.

webview wlan cluster-virtual-ip *virtual-ip-address-of-wlan-cluster*

Syntax Definitions

virtual-ip-address-of-wlan-cluster	Virtual IP address (IPV4) of the AP cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use this command to configure the AP cluster virtual IP address to access the OAW-AP web interface from the webview.

Examples

```
-> webview wlan cluster-virtual-ip 10.25.6.8
```

Release History

Release 6.7.1 R04; command was introduced.

Related Commands

show webview wlan config	Displays the AP cluster virtual IP configured on the switch.

MIB Objects

```
alaIND1WebMgtWlanConfiguredIpAddress
```

webview wlan cluster-virtual-ip precedence

Allows to set the preference for configuring the cluster virtual IP address for webview re-direct. Based on the set preference, the WLAN cluster virtual IP address can be obtained either through configuration or from LLDP packets.

webview wlan cluster-virtual-ip precedence {lldp | configured}

Syntax Definitions

lldp	The preference to obtain the WLAN cluster virtual IP address is set to LLDP packets.
configured	The preference to obtain the WLAN cluster virtual IP address is set to the manually configured WLAN cluster virtual IP address.

Defaults

parameter	default
lldp | configured	lldp

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to set the preference for the cluster virtual IP address for webview re-direct.
- If more than one cluster virtual IP address is obtained through LLDP on the same port, the recently obtained IP is taken into consideration.
- If more than one cluster virtual IP is obtained through LLDP on different ports, the recently obtained IP is taken into consideration.
- If the precedence is set for LLDP obtained IP address, but there is no LLDP obtained cluster virtual IP address, then the configured cluster virtual IP address will be considered if present.
- If the precedence is set for CLI configured cluster virtual IP address, but there is no configured IP address present, then the LLDP obtained cluster virtual IP address will be considered if present.

Examples

```
-> webview wlan cluster-virtual-ip precedence lldp
-> webview wlan cluster-virtual-ip precedence configured
```

Release History

Release 6.7.2.R02; command was introduced.

Related Commands

show webview wlan config	Displays the AP cluster virtual IP configured on the switch.

MIB Objects

`alaIND1WebMgtWlanIpPrecedence`

show webview wlan config

Displays the cluster virtual IP precedence configuration, WLAN AP cluster virtual IP configured on the switch, and WLAN AP cluster virtual IP obtained through LLDP.

show webview wlan config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show webview wlan config
WebView WLAN Cluster-Virtual-IP Precedence = LLDP
WebView WLAN Cluster-Virtual-IP configured address = 0.0.0.0
WebView WLAN Cluster-Virtual-IP LLDP address = 1.1.1.1
```

output definitions

WebView WLAN Cluster-Virtual-IP Precedence	The precedence set for obtaining the cluster virtual IP address of the AP.
WebView WLAN Cluster-Virtual-IP configured address	The manually configured cluster virtual IP address.
WebView WLAN Cluster-Virtual-IP LLDP address	The cluster virtual IP address obtained from the LLDP packets.

Release History

Release 6.7.1.R04; command was introduced.
Release 6.7.2.R02; **WebView WLAN Cluster-Virtual-IP Precedence, WebView WLAN Cluster-Virtual-IP configured address,** and **WebView WLAN Cluster-Virtual-IP LLDP address** output field included.

Related Commands

webview wlan cluster-virtual-ip	Configures the virtual IP address of the Access Point (AP) clusters in the switch.
webview wlan cluster-virtual-ip precedence	Allows to set the preference for the choice of cluster virtual IP address for webview re-direct.

MIB Objects

```
alaIND1WebMgtWlanIpPrecedence
   alaIND1WebMgtWlanConfiguredIpAddressType
   alaIND1WebMgtWlanConfiguredIpAddress
   alaIND1WebMgtWlanLldpIpAddressType
```

9 Configuration File Manager Commands

The Configuration Manager feature allows you to configure your switch using an ASCII-based text file. CLI commands may be typed into a text document—referred to as a *configuration file*—and then uploaded and applied to the switch.

MIB information for the Configuration Manager commands is as follows:

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

A summary of the available commands is listed here:

configuration apply
configuration error-file limit
show configuration status
configuration cancel
configuration syntax check
configuration snapshot
show configuration snapshot
write terminal

configuration apply

Applies a configuration file to the switch. Files may be applied immediately or after a designated timer session. With the timer session option, files are applied either at a scheduled date and time or after a specified period of time (that is, 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 (that is, a countdown) has passed. Values for *hh* range from 00 through 23. Values for *mm* range from 00 through 59.
verbose	When verbose is entered, information is displayed on your workstation's console as each command in the configuration file is applied.

Defaults

By default, **verbose** error checking is not performed.

Platforms Supported

OmniSwitch 6450, 6350

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, that is, 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 results in an error whenever it is applied to the switch through 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, see page 49-47.

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 6.6.1; command was introduced.

Related Commands

configuration syntax check	Performs a syntax and authorization check of all CLI commands contained in a configuration file.

MIB Objects

```
alcatelIND1ConfigMgrMIBObjects
   configFileName
   configFileMode
   configFileAction
   configTimerFileName
   configTimerFileTime
```

configuration error-file limit

Specifies the maximum number of configuration error files allowed in the switch's **/flash** directory. Error files are normally generated when a configuration file is applied to the switch. Error files are identified by their **.err** extension.When the maximum number of **.err** files is exceeded, any new error file overwrites 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 6450, 6350

Usage Guidelines

- When the error file limit is set to 1 (the default value), the next error file generated by the switch replaces 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 automatically removes 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 6.6.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
configuration cancel	Cancels a pending timer session for a configuration file.

MIB Objects

```
alcatelIND1ConfigMgrMIBObjects
   configErrorFileMaximum
```

show configuration status

Displays whether there is a pending timer session scheduled for a configuration file and indicates whether the running configuration and the saved configuration files are *identical* or *different*. This command also displays the number of error files that is held in the flash directory.

show configuration status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- A timer session can be scheduled using the **configuration apply** command. For more information, see page 9-2.
- The screen output **File configuration** *</path/filename>***: scheduled at** *dd/mm hh:mm* indicates that a timer session has been scheduled for a later time.
- The output **No file configuration has been scheduled** indicates an idle timer session (that is, 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** are displayed.
- When the running and saved configurations are the different, the output **Running configuration and saved configuration are different** are displayed.
- To synchronize the running and saved configuration, use the **write memory** command.

Examples

```
-> show configuration status
```

Release History

Release 6.6.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
configuration cancel	Cancels a pending timer session for a configuration file.
configuration error-file limit	Specifies the maximum number of configuration error files allowed in the switch's **/flash** directory.
write memory	Copies the running configuration (RAM) to the working directory.

MIB Objects

```
configTimerFileGroup
   configTimerFileStatus
```

configuration cancel

Cancels a pending timer session for a configuration file.

configuration cancel

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> configuration cancel
```

Release History

Release 6.6.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
show configuration status	Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

```
configTimerFileGroup
   configTimerClear
```

configuration syntax check

Performs a syntax and authorization check of all CLI commands contained in a configuration file.

configuration syntax check *path/filename* **[verbose]**

Syntax Definitions

path/filename	The configuration file being checked for syntax and authorization errors. If a configuration file is located in another directory, be sure to specify the full path. For example, **/flash/working/asc.1.snap**.
verbose	When **verbose** is specified in the command line, all syntax contained in the configuration file is printed to the console, even if no error is detected. When **verbose** is *not* specified in the command line, cursory information (number of errors and error log file name) is printed to the console *only if a syntax or configuration error is detected*.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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* (that is, 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 6.6.1; command was introduced.

Related Commands

configuration apply	Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
show configuration status	Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

```
configFileGroup
   configErrorFileName
   configErrorFileMaximum
   configFileMode
   configFileStatus
```

configuration snapshot

Generates a snapshot file of the switch's non-default current running configuration. A snapshot can be generated for all current network features or for one or more specific network features. A snapshot is a single text file that can be viewed, edited, and reused as a configuration file.

configuration snapshot *feature_list* **[***path/filename***]**

Syntax Definitions

feature_list The description for the network feature(s) to be included in the snapshot. You may enter more than one network feature in the command line. Current snapshot-supported network features are listed below.

snapshot-supported features		
802.1q	**ip**	**pmm**
aaa	**ip-helper**	**policy**
aip	**ip-routing**	**qos**
all	**ipmr**	**rdp**
bridge	**ipms**	**rip**
chassis	**ipv6**	**ripng**
efm-oam	**linkagg**	**session**
erp	**loopback-detection**	**snmp**
ethernet-oam	**module**	**stack-manager**
health	**ntp**	**stp**
interface	**port-mapping**	**vlan**

path/filename A user-defined name for the resulting snapshot file. For example, **test_snmp_snap**. You may also enter a specific path for the resulting file. For example, the syntax **/flash/working/test_snmp_snap** places the **test_snmp_snap** file in the switch's **/flash/working** directory.

Defaults

If a file name is not specified, the default file name **asc.#.snap** is used. Here, # indicates the order in which the default file is generated. For example, the first default file name to be generated is **asc.1.snap**, the second default file name to be generated is named **asc.2.snap**, and so on. By default, all snapshot files are placed in the root **/flash** directory.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.
Release 6.6.2; **erp** parameter added.

Related Commands

N/A

MIB Objects

```
configManager
   configSnapshotFileName
   configSnapshotAction
   configSnapshotAllSelect
   configSnapshotVlanSelect
   configSnapshotSpanningTreeSelect
   configSnapshotQOSSelect
   configSnapshotIPSelect
   configSnapshotIPMSSelect
   configSnapshotAAASelect
   configSnapshotSNMPSelect
   configSnapshot802.1QSelect
   configSnapshotLinkAggregateSelect
   configSnapshotPortMirrorSelect
   configSnapshotXIPSelect
   configSnapshotHealthMonitorSelect
   configSnapshotBootPSelect
   configSnapshotBridgeSelect
   configSnapshotChassisSelect
   configSnapshotInterfaceSelect
   configSnapshotPolicySelect
   configSnapshotSessionSelect
   configSnapshotSystemServiceSelect
   configSnapshotWebSelect
   configSnapshotRIPSelect
   configSnapshotIPRMSelect
   configSnapshotIPMRSelect
   configSnapshotModuleSelect
   configSnapshotRDPSelect
```

```
configSnapshotIPv6Select
```

show configuration snapshot

Displays the switch's current running configuration for all features or for the specified feature(s).

show configuration snapshot [*feature_list***]**

Syntax Definitions

feature_list	Specify the feature(s) for which you want to display the running configuration. List the features separated by a space with no comma.

snapshot-supported features		
802.1q	**ip**	**pmm**
aaa	**ip-helper**	**policy**
aip	**ip-routing**	**qos**
all	**ipmr**	**rdp**
bridge	**ipms**	**rip**
chassis	**ipv6**	**ripng**
efm-oam	**linkagg**	**session**
erp	**loopback-detection**	**snmp**
ethernet-oam	**module**	**stack-manager**
health	**ntp**	**stp**
interface	**port-mapping**	**vlan**

Defaults

By default, this command shows configuration information for *all* features.

Platforms Supported

OmniSwitch 6450, 6350

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
```

AAA output for Case Sensitive MAC address Authentication

```
-> show configuration snapshot aaa
aaa authentication console "local"
user "public" read All write All no auth authkey 391b0e74dbd13973d703cceaa4a8e30
retransmit 3 timeout 2 auth-port 1812 mac-address-format-status enable
mac-address-format 1 lowercase

-> 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
```

Bridging snapshot with finite learning window:

```
-> show configuration snapshot bridge
! Bridging :
port-security SHUTDOWN 1 boot-up disable no-aging disable convert-to-static enable
learn-as-static enable mac-move enable
```

Bridging snapshot with infinite learning window:

```
-> show configuration snapshot bridge
! Bridging :
port-security SHUTDOWN 0 boot-up disable no-aging enable convert-to-static disable
learn-as-static enable mac-move enable
```

Release History

Release 6.6.1; command was introduced.
Release 6.6.2; **erp** parameter added.

Related Commands

write terminal	Displays the switch's current running configuration for all features.

MIB Objects

```
configManager
   configSnapshotFileName
   configSnapshotAction
   configSnapshotAllSelect
   configSnapshotVlanSelect
   configSnapshotSpanningTreeSelect
   configSnapshotQOSSelect
   configSnapshotIPSelect
   configSnapshotIPMSSelect
   configSnapshotAAASelect
   configSnapshotSNMPSelect
   configSnapshot802.1QSelect
   configSnapshotLinkAggregateSelect
   configSnapshotPortMirrorSelect
   configSnapshotXIPSelect
   configSnapshotHealthMonitorSelect
   configSnapshotBootPSelect
   configSnapshotBridgeSelect
   configSnapshotChassisSelect
   configSnapshotInterfaceSelect
   configSnapshotPolicySelect
   configSnapshotSessionSelect
   configSnapshotSystemServiceSelect
   configSnapshotWebSelect
   configSnapshotRIPSelect
   configSnapshotIPRMSelect
   configSnapshotIPMRSelect
   configSnapshotModuleSelect
   configSnapshotRDPSelect
   configSnapshotIPv6Select
```

write terminal

Displays the switch's current running configuration for all features.

write terminal

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

show configuration snapshot	Displays the switch's current running configuration for all features or for the specified feature(s).

MIB Objects

```
configManager
   mib_configSnapshotAllSelect
```

10 SNMP and OpenFlow 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

OpenFlow is a communications interface defined between the control and forwarding layers that is used in a Software Defined Network (SDN). OpenFlow separates the control plane and the data plane in the switch. Traditionally, switches and routers have made decisions on where packets should travel based on rules local to the device. With OpenFlow, only the data plane exists on the switch itself, and all control decisions are communicated to the switch from a central Controller. The OmniSwitch can operate in AOS or OpenFlow mode, including a modified OpenFlow mode known as Hybrid mode.

MIB information for the OpenFlow commands is as follows:

Filename: ALCATEL-IND1-OPENFLOW-MIB.mib
Module: alcatelIND1OpenflowMIB

A summary of the available commands is listed here:

SNMP station commands	**snmp station** **show snmp station**
SNMP community map commands	**snmp community map** **snmp community map mode** **show snmp community map**
SNMP security commands	**snmp security** **show snmp security** **show snmp statistics** **show snmp mib family**
SNMP trap commands	**snmp trap absorption** **snmp trap to webview** **snmp trap replay** **snmp trap filter** **snmp authentication trap** **show snmp trap replay** **show snmp trap filter** **snmp authentication trap** **show snmp trap config**
SNMP View Commands	**snmp view oid-tree** **show snmp views** **show snmp view viewname**
OpenFlow Commands	**openflow back-off-max** **openflow idle-probe-timeout** **openflow logical-switch** **openflow logical-switch controller** **openflow logical-switch interfaces** **show openflow** **show openflow logical-switch** **show openflow logical-switch stats**

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 is sent.
ipv6_address	The IPv6 address to which SNMP unicast traps is 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 6450, 6350

Usage Guidelines

- Use the no form of the command to remove an existing SNMP station.
- When adding an SNMP station, you have to 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 have to 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 has to correspond with the UDP destination port configured at the receiving SNMP station(s).
- When the SNMP station is enabled, the switch transmits traps to the specified IP or IPv6 address.

Examples

```
-> snmp station 168.22.2.2 111 username2 v1 disable
-> snmp station 168.151.2.101 "test lab"
-> snmp station 170.1.2.3 username1 enable
-> snmp station 1.1.2.2 v2
-> no snmp station 2.2.2.2
-> snmp station 300::1 enable
-> no snmp station 300::1
```

Release History

Release 6.6.1; command was introduced.

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 6450, 6350

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 6.6.4; command was introduced

Related Commands

snmp station	Adds a new SNMP station; modifies or deletes an existing SNMP station.

MIB Objects

N/A

show snmp station

Displays the current SNMP station status.

show snmp station

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show snmp station
ipAddress/udpPort                                       status    protocol user
--------------------------------------------------------+---------+--------+------
172.21.160.32/4000                                      enable    v3       abc
172.21.160.12/5000                                      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.
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 6.6.1; 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 has to 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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_username
disabled  test_string3                   cc_username
disabled  test_string4                   jj_username
```

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 6.6.1; 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

NA

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 accepts all SNMP v1, v2, and v3 requests.
authentication set	The switch accepts all requests *except* v1, v2, and non-authenticated v3 set requests. SNMP v1, v2, and non-authenticated v3 set requests is rejected.
authentication all	The switch accepts 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 is rejected.
privacy set	The switch accepts *only* authenticated SNMP v3 get, get-next and encrypted v3 set requests. All other requests is rejected.
privacy all	The switch accepts only encrypted v3 get, get-next, and set requests. All other requests is rejected.
trap only	All SNMP get, get-next, and set requests is rejected.

Defaults

By default, the SNMP security default is set to **privacy all**, which is the highest level of security.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

Refer to the command on page 10-12 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 6.6.1; command was introduced.

Related Commands

snmp security	Configures the SNMP security settings.

MIB Objects

N/A

show snmp statistics

Displays the current SNMP statistics.

show snmp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
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 6450, 6350

Usage Guidelines

- If a table name is not specified in the command syntax, all MIB table names is displayed.
- If the command family is not valid for the entire MIB table, the command family is 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
MIP ID              MIB TABLE NAME TABLE OID                    FAMILY
-------+--------------------------------------+---------------------------------
  6145   alaLbdTrapsObj 1.3.6.1.4.1.6486.800.1.3.2.22.2      NO SNMP ACCESS
  6146   esmConfTrap 1.3.6.1.4.1.6486.800.1.2.1.5.1.1.1      NO SNMP ACCESS
  6147   alaLFPConfigTable 1.3.6.1.4.1.6486.800.1.2.1.5.1.1.2.11 interface
  6148   alaLFPGroupTable 1.3.6.1.4.1.6486.800.1.2.1.5.1.1.2.10 interface
  6149   alaLbdPortConfigTable 1.3.6.1.4.1.6486.800.1.2.1.56.1.1.5.1 lbd
  6150   alaLbdPortStatsTable 1.3.6.1.4.1.6486.800.1.2.1.56.1.1.6.1 lbd
  6152   alaUdldPortConfigTable 1.3.6.1.4.1.6486.800.1.2.1.44.1.1.6.1 interface
..
..
..
..
..
173059   alaRadAuthorTable 1.3.6.1.4.1.6486.800.1.2.1.73.1.1.1.1 radius
173060   alaRadByodTable 1.3.6.1.4.1.6486.800.1.2.1.73.1.1.1.4 radius
173061   alaRadGlobalTable 1.3.6.1.4.1.6486.800.1.2.1.73.1.1.1.5 radius
```

```
-> show snmp mib family trapStationTable
MIP ID   MIB TABLE NAME            TABLE OID                              FAMILY
-------+-----------------+--------------------------------------+---------
73735   trapStationTable   1.3.6.1.4.1.6486.800.1.2.1.2.1.1.1.2       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 6.6.1; command was introduced.
Release 6.7.2.R04; extended to display the oid of the Table/objects.

Related Commands

show snmp trap filter	Displays the SNMP trap filter information.

MIB Objects

```
N/A
```

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 is 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.Trap absorption drops additional traps within the absorption period (default 15 seconds).

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 are replayed from the switch.
ipv6_address	The IPv6 address for the SNMP station to which traps are replayed from the switch.
seq_id	The sequence number from which trap replay begins. 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, and so on. If no sequence number is entered, all stored traps are replayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **show snmp station** command on page page 10-6 to display the latest stored sequence number for each SNMP station.
- The switch replays traps in the same order that they were previously sent, beginning from the specified sequence number.
- When traps are replayed, the original dates on which the trap was issued, rather than the current dates are used.
- If the specified sequence number is lower than the oldest trap sequence number stored in the switch, the switch replays all stored traps.
- If the specified sequence number is equal to or greater than the oldest trap sequence number stored, the switch replays all stored traps from the specified sequence number up to the latest sequence number.
- If the specified sequence number is greater than the latest sequence number, no traps are replayed.

Examples

```
-> snmp trap replay 172.12.2.100
-> snmp trap replay 300::1
```

Release History

Release 6.6.1; command was introduced.

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 is 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 6450, 6350

Usage Guidelines

- To *enable* trap filtering, use the syntax **snmp trap filter** *ip_address trap_id_list.*
- To *disable* trap filtering, use the syntax **no snmp trap filter** *ip_address trap_id_list*.
- When filtering is enabled, the specified trap(s) *is not* sent to the SNMP station. When filtering is disabled, the specified traps *is* sent to the SNMP station.
- To display a list of traps and their ID numbers, use the **show snmp trap config** command.

Examples

```
-> snmp trap filter 172.1.2.3 1
-> snmp trap filter 172.1.2.3 0 1 3 5
-> snmp trap filter 300::1 1 3 4
-> no snmp trap filter 172.1.2.3 1
-> no snmp trap filter 172.1.2.3 0 1 3 5
-> no snmp trap filter 300::1 1 3
```

Release History

Release 6.6.1; command was introduced.

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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> snmp authentication trap enable
-> snmp authentication trap disable
```

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

A maximum of 60 traps is replayed.

Examples

```
-> show snmp trap replay
ipAddress                                  oldest replay number
-----------------------------------------+--------------------
172.21.160.32                                          12
172.21.160.12                                          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.
Oldest Replay Number	Number of the oldest replayed trap.

Release History

Release 6.6.1; 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 6450, 6350

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
-----------------------------------------+-----------------------------------
172.21.160.32                                1   3   4
172.21.160.12                              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.
TrapId List	Identification number for the traps being filtered.

Release History

Release 6.6.1; 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 (that is, enable or disable).

show snmp authentication trap

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show snmp authentication trap
snmp authentication trap = disable
```

Release History

Release 6.6.1; 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 6450, 6350

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
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 6.6.1; 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
```

snmp view oid-tree

Use this command to create or remove an SNMP view with include or exclude option. Use **No** form of this command to remove the entire SNMP view or specific OID (tree) from the view.

snmp view *viewname* **oid-tree {include | exclude}**

no snmp view *viewname* **oid-tree**

Syntax Definitions

viewname	Specifies name of the view to be created or modified. Maximum length of view name is 32 character.
oid-tree	Specifies OID information to be added or removed in the view. Maximum OID length is 64 character.
include	Creates an SNMP view with include option.
exclude	Creates an SNMP view with exclude option.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This view list can be modified or deleted only by the admin user. This view is integrated with the user as read-only/ read-write by using the **user** command.
- An SNMP View has to be created with specific OID for the view.
- When an OID tree is created with **include** option, only the OID and OID tree (if any) below this OID has privilege to access the switch. OIDs other than these are excluded by default.
- When an OID tree is created with **exclude** option, OID and OID tree (if any) below this OID have no privilege to access the switch. OIDs other than these are included by default.
- A maximum 10 views can be created on the switch.

Examples

```
-> snmp view test 1.3.6.1.4.1.6486.800.1.2.1.5.1.1.2.10 exclude
-> snmp view ip_test 1.3.6.1.4.1.6486.800.1.2.1.23.1.1.14.1 include
-> no snmp view management
-> no snmp view remote_client 1.3.6.1.2.1.2.2.1
```

Release History

Release 6.7.2.R04; command was introduced.

Related Commands

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.
show snmp views	Displays the list of SNMP views created with the type.
show snmp view viewname	Displays the list of OID for a particular view.

MIB Objects

```
snmpAgtViewMIB
   snmpAgtViewTable
```

show snmp views

Displays the list of SNMP views created with the type.

show snmp views

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use this command to display the list of SNMP views created with the view type.

Examples

```
-> show snmp views
VIEW NAME                          VIEW TYPE
-----------------------------------+-----------
remote_read                         EXCLUDE
remote_write                        EXCLUDE
```

output definitions

VIEW NAME	Displays the name of the view name.
VIEW TYPE	Displays the name of view type.

Release History

Release 6.7.2.R04; command was introduced.

Related Commands

snmp view oid-tree	Use this command to create or remove an SNMP view with include or exclude option. Use **No** form of this command to remove the entire SNMP view or specific OID (tree) from the view.
show snmp view viewname	Displays the list of OID for a particular view.
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.

MIB Objects

```
snmpAgtViewMIB
   snmpAgtViewEntry
```

show snmp view viewname

Displays the list of OID for a particular view.

show snmp view *viewname*

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show snmp view lfp_read
View Name : lfp_read                          View Type : EXCLUDE
OID LIST                                      TABLE/OBJECT NAME
----------------------------------------------------------+-----------
1.3.6.1.4.1.6486.800.1.2.1.5.1.1.2.11.1.3  alaLFPConfigRowStatus
1.3.6.1.4.1.6486.800.1.2.1.3.1.1.1.1           vlanTable
```

output definitions

OID LIST	Displays the OID list.
TABLE/OBJECT NAME	Displays the name of Table or Object.

Release History

Release 6.7.2.R04; command was introduced.

Related Commands

snmp view oid-tree	Use this command too create or remove an SNMP view with include or exclude option. Use **No** form of this command to remove the entire SNMP view or specific OID (tree) from the view.
show snmp views	Displays the list of SNMP views created with the type.
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.

MIB Objects

```
snmpAgtViewMIB
   snmpAgtViewName
```

openflow back-off-max

Configures the maximum amount of time to wait between Controller connection attempts.

openflow back-off-max *seconds*

Syntax Definitions

seconds	The back-off-max value, in seconds. The valid range is from 1 - 60.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> openflow back-off-max 32
-> openflow back-off-max 60
```

Release History

Release 6.6.5; command introduced

Related Commands

show openflow	Displays global OpenFlow configuration parameters.

MIB Objects

```
alaOpenflowGlobalBackoffMax
```

openflow idle-probe-timeout

Configures the idle probe timeout value.

openflow idle-probe-timeout *seconds*

Syntax Definitions

seconds	The idle probe timeout value, in seconds. The valid range is 0 - 60.

Defaults

parameter	default
seconds	15

Platforms Supported

OmniSwitch 6450

Usage Guidelines

If set to 0, idle probing is disabled.

Examples

```
-> openflow idle-probe-timeout 0
-> openflow idle-probe-timeout 15
-> openflow idle-probe-timeout 60
```

Release History

Release 6.6.5; command introduced

Related Commands

show openflow	Displays global OpenFlow configuration parameters.

MIB Objects

```
alaOpenflowGlobalIdleProbeTimeout
```

openflow logical-switch

Configures an OpenFlow Logical Switch. An OpenFlow Logical Switch consists of a portion of the switch's resources that are managed by an OpenFlow Controller (or set of Controllers) via the OpenFlow Agent.

openflow logical-switch *name* **[admin-state {enable | disable}] [mode {normal | api}] [version {1.0 | 1.3.1}+] [vlan** *vlan_id***]**

no openflow logical-switch <*name*>

Syntax Definitions

name	The Logical Switch name (up to 32 characters).
admin-state enable	Enables the Logical Switch.
admin-state disable	Disables the Logical Switch.
normal	Configures the Logical Switch to run in Normal Mode.
api	Configures the Logical Switch to run in Hybrid (API) Mode. Only one (1) Logical Switch can be configured in Hybrid Mode.
1.0	Configures the Logical Switch to run OpenFlow Version 1.0.
1.3.1	Configures the Logical Switch to run OpenFlow Version 1.3.1.
vlan_id	The Default VLAN for all ports assigned to the Logical Switch. Traffic on this VLAN on these ports will not carry an 802.1q tag. Traffic on all other VLANs on these ports will carry an 802.1q tag. The valid range is 2 - 4093.

Defaults

parameter	default
enable | disable	enable
normal | api	normal
1.0 | 1.3.1	1.0 1.3.1

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Up to three (3) OpenFlow Logical Switches can be configured on an OmniSwitch.
- Use the no form of the command to delete an OpenFlow Logical Switch and all Controller/port configurations for that Logical Switch.
- When a Logical Switch is disabled, all Controllers for that Logical Switch are operationally disabled, and flows added by those Controllers are removed.

- In Normal Mode, the switch operates as per the OpenFlow standards. In Hybrid mode, OpenFlow operates as an interface through which the Controller may add over-ride policies to the switch much like QoS. In Hybrid mode, no traffic is forwarded to the Controller(s) and AOS operates normally.
- OpenFlow versions 1.0 and 1.3.1 are both enabled by default. At least one version must be enabled.
- "vlan" is not valid if the configured mode for the Logical Switch is API. An API Logical Switch implicitly operates on all ports, link aggregates, and VLANs not assigned to other OpenFlow Logical Switches.

Examples

```
-> openflow logical-switch vswitch1
-> openflow logical-switch vswitch1 admin-state enable
-> openflow logical-switch vswitch1 mode normal version 1.0 vlan 5
-> no openflow logical-switch vswitch1
```

Release History

Release 6.6.5; command introduced

Related Commands

show openflow logical-switch	Displays information about all of the configured OpenFlow Logical Switches.

MIB Objects

```
alaOpenflowLogicalSwitchTable
   alaOpenflowLogicalSwitch
   alaOpenflowLogicalSwitchAdminState
   alaOpenflowLogicalSwitchMode
   alaOpenflowLogicalSwitchVersions
   alaOpenflowLogicalSwitchVlan
```

openflow logical-switch controller

Configures a Controller for an OpenFlow Logical Switch. You can configure up to three (3) Controllers per Logical Switch.

openflow logical-switch *name* **controller** *ip_address* **[***:port***] admin-state {enable | disable}**

no openflow logical-switch *name* **controller** *ip_address* **[***:port***]**

Syntax Definitions

name	The Logical Switch name (up to 32 characters).
ip_address	The IP address of Controller.
port	The Controller IP Port (1 - 65535).
enable	Enables the connection to the Controller.
disable	Disables the connection to the Controller.

Defaults

parameter	default
port	6633
enable | disable	enable

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Currently, only IPv4 addresses are supported.
- If a Logical Switch cannot connect to any of its Controllers, it runs in “Fail Secure Mode”. All flow aging, etc. continues unaffected while the Controllers are disconnected.

Examples

```
-> openflow logical-switch vswitch1 controller 1.2.3.4
-> openflow logical-switch vswitch1 controller 1.2.3.4:6634 admin-state enable
-> no openflow logical-switch vswitch1 controller 1.2.3.4
```

Release History

Release 6.6.5; command introduced.

Related Commands

show openflow logical-switch	Displays information about all of the configured OpenFlow Logical Switches.

MIB Objects

```
alaOpenflowControllerTable
   alaOpenflowControllerLogicalSwitch
   alaOpenflowControllerIpType
   alaOpenflowControllerIp
   alaOpenflowControllerPort
   alaOpenflowControllerAdminState
```

openflow logical-switch interfaces

Configures a range of interfaces to/from a Logical Switch.

openflow logical-switch *name* **interfaces {port** *slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

no openflow logical-switch *name* **interfaces {port** *slot/port1***[**-*port2***] | linkagg** *agg_id***[**-*agg_id2***]}**

Syntax Definitions

name	The Logical Switch name (up to 32 characters).
*slot/port***[**-*port2***]**	The slot and port number. Use a hyphen to specify a range of ports (1/1-8).
*agg_id***[**-*agg_id2***]**	The link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> openflow logical-switch vswitch1 interfaces port 1/1
-> no openflow logical-switch vswitch1 interfaces port 1/1
-> openflow logical-switch vswitch2 interfaces linkagg 5
-> no openflow logical-switch vswitch2 interfaces linkagg 5
-> openflow logical-switch vswitch1 interfaces port 1/1-8
-> no openflow logical-switch vswitch1 interfaces port 1/1-8
```

Release History

Release 6.6.5; command introduced

Related Commands

show openflow logical-switch	Displays information about all of the configured Logical Switches.

MIB Objects

```
alaOpenflowInterfaceTable
   alaOpenflowInterfaceLogicalSwitch
   alaOpenflowInterface
```

show openflow

Displays global OpenFlow configuration parameters.

show openflow

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show openflow
Back-off Max       : 60,
Idle Probe Timeout : 15
```

output definitions

Back-off Max	The configured maximum back off time, in seconds, for Controller connection attempts (Range = 1 - 60, Default = 60).
Idle Probe Timeout	The configured idle probe timeout value, in seconds (Range = 1– 60, Default = 15).

Release History

Release 6.6.5; command introduced

Related Commands

openflow back-off-max	Configures the maximum amount of time allowed for Controller connection attempts.
openflow idle-probe-timeout	Configures the idle probe timeout value.

MIB Objects

```
alaOpenflowGlobalBackoffMax
alaOpenflowGlobalIdleProbeTimeout
```

show openflow logical-switch

Displays information about configured OpenFlow Logical Switches.

show openflow logical-switch [*name* **| controllers | interfaces]**

Syntax Definitions

name	The Logical Switch name (up to 32 characters).
controllers	The controllers assigned to this logical switch.
interfaces	The interfaces assigned to this logical switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Enter a Logical Switch name to display only information about a specific Logical Switch.

Examples

```
-> show openflow logical-switch

                         Admin
       Logical Switch    State  Mode    Versions    VLAN   Ctrlrs   Intf   Flows
-------------------------+-----+------+-----------+------+--------+------+-------
vswitch1                  Ena   Norm   1.0             1       1      4       0
vswitch2                  Dis   Norm   1.0, 1.3.1      5       3      4       2
vswitch3                  Ena   API    1.0, 1.3.1    N/A       1      0       0
```

output definitions

Logical Switch	The Logical Switch name
Admin State	The Logical Switch administrative state (Enabled/Disabled).
Mode	The Logical Switch operational Mode (Normal/API).
Versions	The OpenFlow versions enabled on the Logical Switch (1.0/1.3.1).
VLAN	The default VLAN for all ports assigned to the Logical Switch. Zero (0) indicates no VLAN configured.
Ctrlrs	The number of Controllers configured for the Logical Switch (up to three (3) Controllers can be configured per Logical Switch.
Intf	The number of interfaces (ports and link aggregations) configured for the Logical Switch.
Flows	The number of flows pushed to the Logical Switch by its Controllers.
Controller	The controller IP address and port.

output definitions

Role	Current role of the controller. Equal, Master, or Slave.
Oper State	Current connection state of the controller (invalid, operDisabled, sendError, init, connecting, backoff, exchangingHello, active, idle, disconnected).

Release History

Release 6.6.5; command introduced

Related Commands

openflow logical-switch	Configures an OpenFlow Logical Switch.
openflow logical-switch controller	Configures a Controller for an OpenFlow Logical Switch. You can configure up to three (3) Controllers per Logical Switch.
openflow logical-switch interfaces	Configures a range of interfaces to/from a Logical Switch.

MIB Objects

```
alaOpenflowLogicalSwitchTable
   alaOpenflowLogicalSwitch
   alaOpenflowLogicalSwitchAdminState
   alaOpenflowLogicalSwitchMode
   alaOpenflowLogicalSwitchVersions
   alaOpenflowLogicalSwitchVlan
   alaOpenflowLogicalSwitchControllerCount
   alaOpenflowLogicalSwitchInterfaceCount
   alaOpenflowLogicalSwitchFlowCount
```

show openflow logical-switch stats

Displays information about statistics for OpenFlow Logical Switches.

show openflow logical-switch *name* **{flowtable | flowentry | openflowport | group} stats**

Syntax Definitions

name	The Logical Switch name.
flowtable	Display statistics on the flow tables.
flowentry	Display statistics for individual flows.
openflowport	Display statistics for an individual port.
group	Display statistics for groups.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show openflow logical-switch LS1 flowtable stats
   Table                          Flow Count
--------------------------------+---------------
Exact Match Table                  45
Wild card Match Table              32


-> show openflow logical-switch LS1 flowentry stats
   Flow-id                   Received Packets   Received bytes   Duration in sec
---------------------------+------------------+-----------------+-----------------
1                             45                1200                50
2                             32                5000                120

-> show openflow logical-switch LS1 openflow-port stats
   OpenFlow Port            Transmitted Packets   Received Packets Duration in sec
---------------------------+--------------------+--------------------+----------
1/1                           45                1200                 50
1/2                           32                5000                 120

-> show openflow logical-switch LS1 group stats
   Group-id                     Duration in sec
--------------------------------+---------------
       1                                45
       2                                32
```

output definitions

Table	Table type match.
Flow Count	The number of flows matched for the table.
Flow-id	The flow identifier.
Received packets/bytes	The number of packets/bytes received from the flow.
Duration in sec	The number of seconds the flow has been active.
OpenFlow Port	The port on which the flow was received.
Transmitted /received packets	The number of packets transmitted by the flow.
Group-id	The group identifier.

Release History

Release 6.6.5; command introduced

Related Commands

openflow logical-switch	Configures an OpenFlow Logical Switch.
openflow logical-switch controller	Configures a Controller for an OpenFlow Logical Switch. You can configure up to three (3) Controllers per Logical Switch.
openflow logical-switch interfaces	Configures a range of interfaces to/from a Logical Switch.

MIB Objects

N/A

11 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 fails 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 6450, 6350

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 6.6.1; 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***]]**

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 is 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 is 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.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 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
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ip domain-lookup	Enables or disables the DNS resolver.
ip domain-name	Sets or deletes the default domain name for DNS lookups.
show dns	Displays the current DNS resolver configuration and status.

MIB Objects

```
systemDNS
   systemDNSNsAddr1
   systemDNSNsAddr2
   systemDNSNsAddr3
```

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 is 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 is 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> 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 6.6.1; 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	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
```

12 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**
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** **show linkagg accounting** **show linkagg counters** **show linkagg traffic** **linkagg no l2-statistics**

static linkagg size

Creates a static aggregate group between two switches. A static aggregate group contains static links.

static linkagg *agg_num* **size** *size* **[name** *name***] [admin state {enable | disable}]**

no static linkagg *agg_num*

Syntax Definitions

agg_num	The number corresponding to the static aggregate group. Can be an unique integer in the range 0–31.
size	The maximum number of links allowed in the aggregate group. Values can be 2, 4, or 8.
name	The name of the static aggregate group. Can be any alphanumeric string up to 255 characters long. Spaces can be given within quotes (for example, “Static Group 1”).
enable	Specifies that the static aggregate group is active and is able to aggregate links.
disable	Specifies that the static aggregate group is inactive and not able to aggregate links.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6450, 6350

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.
- A maximum of 256 link aggregation ports are supported. The number of link aggregation ports per group determines the maximum number of groups that can be configured. The following table 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, delete them with the **static agg agg num** command before you can delete it.

- Use the **lacp linkagg size** command to create a dynamic aggregation (LACP) group. See page 12-9 for more information about this command.

Examples

```
-> static linkagg 3 size 8
-> static linkagg 4 size 2 admin state disable
-> no static linkagg 3
```

Release History

Release 6.6.1; command introduced.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) link aggregate groups.

MIB Objects

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggSize
   alclnkaggAggLacpType
   alclnkaggAggName
   alclnkaggAggAdminState
```

static linkagg name

Configures a name for an existing static aggregate group.

static linkagg *agg_num* **name** *name*

static linkagg *agg_num* **no name**

Syntax Definitions

agg_num	The number corresponding to the static aggregate group.
name	The name of the static aggregation group, an alphanumeric string up to 255 characters. Spaces can be given within quotes (for example, “Static Group 1”).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command 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 6450, 6350

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 6.6.1; command 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 initially uses 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 6450, 6350

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 can 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 need not 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 configuration. See "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 6.6.1; command introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
show linkagg port	Displays information about link aggregation ports.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortLacpType
   alclnkaggAggPortSelectedAggNumber
```

lacp linkagg size

Creates a dynamic aggregate group that uses the Link Aggregation Control Protocol (LACP) to establish and maintain link aggregation. The **size** parameter is required to create the link aggregate group.

lacp linkagg *agg_num* **size** *size*
[name *name***]**
[admin state {enable | disable}]
[actor admin key *actor_admin_key***]**
[actor system priority *actor_system_priority***]**
[actor system id *actor_system_id***]**
[partner system id *partner_system_id***]**
[partner system priority *partner_system_priority***]**
[partner admin key *partner_admin_key***]**

no lacp linkagg *agg_num*

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group. Can be a unique integer in the range 0–31.
size	The maximum number of links that can belong to the aggregate. Values can be 2, 4, or 8.
name	The name of the dynamic aggregate group. Can be any alphanumeric string up to 255 characters long. Spaces must be contained within quotes (for example, “Dynamic Group 1”).
enable	Specifies that the dynamic aggregate group is active and is able to aggregate links.
disable	Specifies that the dynamic aggregate group is inactive and not able to aggregate links.
actor_admin_key	The administrative key value associated with the dynamic aggregate group. Possible values are 0–65535.
actor_system_priority	The priority of the dynamic aggregate group. Possible values are 0–65535.
actor_system_id	The MAC address of the dynamic aggregate group on the switch.
partner_system_id	The MAC address of the remote system to which the aggregate group of the switch is attached.
partner_system_priority	The priority of the remote system to which the aggregate group is attached. Possible values are 0–65535.
partner_admin_key	The administrative key for the remote partner of the aggregate group. Possible values are 0–65535.

Defaults

parameter	default
enable | disable	enable

Platforms Supported

OmniSwitch 6450, 6350

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.
- A maximum of 256 link aggregation ports are supported. The number of link aggregation ports per group determines the maximum number of groups that can be configured. The following table 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, disable the group with the **lacp linkagg admin state** command before you can delete it.
- Optional parameters for the dynamic aggregate group can be configured when the aggregate is created or the dynamic aggregate group can be modified later.
- Use the **static linkagg size** command to create static aggregate groups. See page 12-3 for more information about this command.

Examples

```
-> lacp linkagg 2 size 4
-> lacp linkagg 3 size 2 admin state disable actor system priority 65535
```

Release History

Release 6.6.1; command introduced.

Related Commands

show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

`alclnkaggAggTable`

```
alclnkaggAggNumber
alclnkaggAggSize
alclnkaggAggLacpType
alclnkaggAggName
alclnkaggAggAdminState
alclnkaggAggActorAdminKey
alclnkaggAggActorSystemPriority
alclnkaggAggActorSystemID
alclnkaggAggPartnerSystemID
alclnkaggAggPartnerSystemPriority
alclnkaggAggPartnerAdminKey
```

lacp linkagg name

Configures a name for a dynamic aggregate group.

lacp linkagg *agg_num* **name** *name*

lacp linkagg *agg_num* **no name**

Syntax Definitions

agg_num	The number corresponding to the dynamic aggregate group.
name	The name of the dynamic aggregate group. Can 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 6450, 6350

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 6.6.1; command 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 6450, 6350

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 6.6.1; command 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 1–65535.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command 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 dynamic aggregate group of the switch in relation to other aggregate groups. Possible values are 0–65535.

Defaults

parameter	default
actor_system_priority	0

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command 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 6450, 6350

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 6.6.1; command 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 dynamic aggregate group of the local switch 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 6450, 6350

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* specifies the priority of remote system.

Examples

```
-> lacp linkagg 2 partner system id 00:20:da4:32:81
-> lacp linkagg 2 no partner system id
```

Release History

Release 6.6.1; command 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 6450, 6350

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 6.6.1; command 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 6450, 6350

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 6.6.1; command 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 initially uses 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 12-25.
actor_system_id	The MAC address of this dynamic aggregate group on the switch.
actor_system_priority	The priority of the dynamic aggregate group. Possible values are 0–255.
partner_admin_system_id	The MAC address of the remote switch's dynamic aggregate group.
partner_admin_key	The administrative key for the dynamic aggregation group's remote partner. Possible values are 0–65535.
partner_admin_system_priority	The priority of the remote system to which the dynamic aggregation group is attached. Possible values are 0–255.
partner admin state	See the **lacp agg partner admin state** command on page 12-31.
actor_port_priority	The priority of the actor port. Possible values are 0–255.
partner_admin_port	The administrative state of the partner port. Possible values are 0–65535.
partner_admin_port_priority	The priority of the partner port. Possible values are 0–255.

Defaults

parameter	default
[active] [timeout]....	active, timeout, aggregate

Platforms Supported

OmniSwitch 6450, 6350

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 can 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 need not be configured sequentially and can be on any Network Interface (NI).
- The **ethernet**, **fastethernet**, and **gigaethernet** keywords do not modify port configuration. See "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 6.6.1; command introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays information about ports associated with a particular aggregate group or all aggregates.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggActorAdminKey
   alclnkaggAggPortLacpType
   alclnkaggAggPortActorAdminState
   alclnkaggAggPortActorSystemID
   alclnkaggAggPortActorSystemPriority
   alclnkaggAggPortPartnerAdminSystemID
   alclnkaggAggPortPartnerAdminKey
   alclnkaggAggPortPartnerAdminSystemPriority
   alclnkaggAggPortPartnerAdminState
```

```
alclnkaggAggPortActorPortPriority
alclnkaggAggPortPartnerAdminPort
alclnkaggAggPortPartnerAdminPortPriority
```

lacp agg actor admin state

Configures the system administrative state of the slot and port for the dynamic aggregate group on the local switch. The state values correspond to bits in the actor state octet in the LACPDU frame.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **actor admin state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}**

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port*
actor admin state {[[no] active] [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] | none}

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch initially uses 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 6450, 6350

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 port configuration. See "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 6.6.1; command 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 (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 initially uses 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 6450, 6350

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 configuration. See "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 6.6.1; command 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 initially uses 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 6450, 6350

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 configuration. See "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 6.6.1; command 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 initially uses 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 6450, 6350

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 configuration. See "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 6.6.1; command 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 initially uses 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 6450, 6350

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 configuration. See "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 6.6.1; command 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 initially uses 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 6450, 6350

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 configuration. See "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 6.6.1; command introduced.

Related Commands

lacp linkagg size	Creates a dynamic aggregate group.
show linkagg port	Displays detailed information about ports associated with a particular aggregate group or all aggregate groups.
show linkagg port	Displays information about slots and ports associated with all aggregate groups.

MIB Objects

```
AlcLnkAggAggPortTable
   alclnkaggAggPortGlobalPortNumber
   alclnkaggAggPortPartnerAdminKey
```

lacp agg partner admin system priority

Configures the partner system priority for a dynamic aggregate group port.

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **partner admin system priority** *partner_admin_system_priority*

lacp agg [ethernet | fastethernet | gigaethernet] *slot/port* **no partner admin system priority**

Syntax Definitions

ethernet	Documents that the port is 10 Mbps Ethernet.
fastethernet	Documents that the port is 100 Mbps Fast Ethernet.
gigaethernet	Documents that the port is Gigabit Ethernet.
slot	The slot number for this aggregate.
port	The port that the switch initially uses 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 6450, 6350

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 configuration. See "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 6.6.1; command 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 initially uses 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 6450, 6350

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 configuration. See "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 6.6.1; command 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 initially uses 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

Platforms Supported

OmniSwitch 6450, 6350

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 configuration. See "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 6.6.1; command 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 initially uses 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 6450, 6350

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 configuration. See "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 6.6.1; command 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
```

show linkagg

Displays information about static and dynamic (LACP) aggregate groups.

show linkagg [*agg_num***]**

Syntax Definitions

agg_num	Specifies the aggregate group. Configured through the **static linkagg size** or **lacp linkagg size** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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
Number  Aggregate  SNMP Id  Size  Admin State  Oper State     Att/Sel Ports
-------+----------+--------+----+-------------+-------------+-------------
   1     Static    40000001   8    ENABLED      UP             2   2
   2     Dynamic   40000002   4    ENABLED      DOWN           0   0
   3     Dynamic   40000003   8    ENABLED      DOWN           0   2
   4     Dynamic   40000004   8    ENABLED      UP             3   3
   5     Static    40000005   2    DISABLED     DOWN           0   0
```

Output fields are defined here:

output definitions

Number	The aggregate group number.
Aggregate	The type of aggregate group, which can be **Static** or **Dynamic**.
SNMP Id	The SNMP ID associated with the aggregate group.
Size	The number of links in this aggregate group.

output definitions (continued)

Admin State	The current administrative state of the aggregate group, which can be **ENABLED** or **DISABLED**. You can modify this parameter with the **static linkagg admin state** command (see page 12-6) for static aggregate groups and with the **lacp linkagg admin state** command (see page 12-13) for dynamic aggregate groups.
Oper State	The current operational state of the aggregate group, which can be **UP** or **DOWN**.
Att Ports	The number of ports attached to this aggregate group.
Sel Ports	The number of ports that could possibly attach to the aggregate group.

A static aggregate is specified:

```
-> show linkagg 5
Static Aggregate
  SNMP Id                  : 40000005,
  Aggregate Number         : 5,
  SNMP Descriptor          : Omnichannel Aggregate Number 5 ref 40000005 size 2,
  Name                     : AGG5,
  Admin State              : ENABLED,
  Operational State        : DOWN,
  Aggregate Size           : 2,
  Number of Selected Ports : 0,
  Number of Reserved Ports : 0,
  Number of Attached Ports : 0,
  Primary Port             : NONE
```

output 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 12-5).
Admin State	The administrative state of this static aggregate group, which can be **ENABLED** or **DISABLED**. You can modify this parameter with the **static linkagg admin state** command (see page 12-6).
Operational State	The operational state of this static aggregate group, which can be **UP** or **DOWN**.
Aggregate Size	The number of links configured for this static aggregate group.
Number of Selected Ports	The number of ports that could possibly attach to this static aggregate group.
Number of Reserved Ports	The total number of ports reserved for use in link aggregation by this static aggregate group. (**Note**: This field is not relevant for static aggregate groups.)
Number of Attached Ports	The number of ports attached to this static aggregate group.
Primary Port	The port number of the first port to join this static aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.

A dynamic aggregate group is specified:

```
-> show linkagg 2
Dynamic Aggregate
  SNMP Id                   : 40000002,
  Aggregate Number          : 2,
  SNMP Descriptor           : Dynamic Aggregate Number 2 ref 40000002 size 4,
  Name                      : AGG 2,
  Admin State               : ENABLED,
  Operational State         : DOWN,
  Aggregate Size            : 4,
  Number of Selected Ports  : 0,
  Number of Reserved Ports  : 0,
  Number of Attached Ports  : 0,
  Primary Port              : NONE,
LACP
  MACAddress                : [00:1f:cc:00:00:00],
  Actor System Id           : [00:20:da:81:d5:b0],
  Actor System Priority     : 50,
  Actor Admin Key           : 120,
  Actor Oper Key            : 0,
  Partner System Id         : [00:20:da:81:d5:b1],
  Partner System Priority   : 70,
  Partner Admin Key         : 220,
  Partner Oper Key          : 0
  Pre-emption               : ENABLED
  Pre-empt Value            : 250
```

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 12-12).
Admin State	The administrative state of this dynamic aggregate group, which can be **ENABLED** or **DISABLED**. You can modify this parameter with the **lacp linkagg admin state** command (see page 12-13).
Operational State	The operational state of this dynamic aggregate group, which can be **UP** or **DOWN**.
Aggregate Size	The number of links configured for this dynamic aggregate group.
Number of Selected Ports	The number of ports available to this dynamic aggregate group.
Number of Reserved Ports	The total number of ports reserved for use in link aggregation by this dynamic aggregate group.
Number of Attached Ports	The number of ports 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 12-17).

output definitions (continued)

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 12-16).
Actor Admin Key	The administrative key associated with this dynamic aggregate group. You can modify this parameter with the **lacp linkagg actor admin key** command (see page 12-15).
Actor Oper Key	The operational key associated with this dynamic aggregate group.
Partner System Id	The MAC address of the remote dynamic aggregate group. You can modify this parameter with the **lacp linkagg partner system id** command (see page 12-18).
Partner System Priority	The priority of the remote system to which this dynamic aggregation group is attached. You can modify this parameter with the **lacp linkagg partner system priority** command (see page 12-20).
Partner Admin Key	The administrative key for this dynamic aggregation group's remote partner. You can modify this parameter with the **lacp linkagg partner admin key** command (see page 12-21).
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.

Release History

Release 6.6.3; command introduced.

Related Commands

static linkagg size	Creates a static aggregate group.
lacp linkagg size	Creates a dynamic aggregate group.

MIB Objects

```
alclnkaggAggTable
   alclnkAggSize
   alclnkaggAggNumber
   alclnkaggAggDescr
   alclnkaggAggName
   alclnkaggAggLacpType
   alclnkaggAggAdminState
   alclnkaggAggOperState
   alclnkaggAggNbrSelectedPorts
   alclnkaggAggNbrAttachedPorts
   alclnkaggPrimaryPortIndex
   alclnkaggAggMACAddress
   alclnkaggAggActorSystemPriority
   alclnkaggAggActorSystemID
   alclnkaggAggPartnerAdminKey
   alclnkaggAggActorAdminKey
   alclnkaggAggActorOperKey
   alclnkaggAggPartnerSystemID
   alclnkaggAggPartnerSystemPriority
   alclnkaggAggPartnerOperKey
   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 6450, 6350

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 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 the port is the primary port in the link agg.
Standby	Whether 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 **show linkagg** 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.

output definitions (continued)

Actor System Id	The actor system ID (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.
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 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 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 configure aggregation. Configured through the **lacp agg partner admin port** command.
Partner Oper Port	The operational port number assigned to the port by the protocol partner of the port.
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 configure aggregation. Configured through the **lacp agg partner admin port priority** command.
Partner Oper Port Priority	The priority value assigned to the 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.

output definitions (continued)

Partner Admin State	The administrative state of the partner's port. Configured through the **lacp agg partner admin state** command.
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 **show linkagg** command.

Release History

Release 6.6.3; command introduced.

Related Commands

static agg agg num	Configures a slot and port for a static aggregate group.
lacp agg actor admin key	Configures a slot and port for a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggPortTable
   alclnkaggAggPortActorSystem
   alclnkaggAggPortActorSystemPriority
   alclnkaggAggPortActorSystemID
   alclnkaggAggPortActorAdminKey
   alclnkaggAggPortActorOperKey
   alclnkaggAggPortPartnerAdminSystemPriority
   alclnkaggAggPortPartnerOperSystemPriority
   alclnkaggAggPortPartnerAdminSystemID
   alclnkaggAggPortPartnerOperSystemID
   alclnkaggAggPortPartnerAdminKey
   alclnkaggAggPortPartnerOperKey
   alclnkaggAggPortSelectedAggID
   alclnkaggAggPortAttachedAggID
   alclnkaggAggPortActorPort
   alclnkaggAggPortActorPortPriority
   alclnkaggAggPortPartnerAdminPort
   alclnkaggAggPortPartnerOperPort
   alclnkaggAggPortPartnerAdminPortPriority
   alclnkaggAggPortPartnerOperPortPriority
   alclnkaggAggPortActorAdminState
   alclnkaggAggPortActorOperState
   alclnkaggAggPortPartnerAdminState
   alclnkaggAggPortPartnerOperState
   alclnkaggAggPortStandbyState
```

show linkagg accounting

Displays statistics collected for packets transmitted and received on link aggregate ports.

show linkagg *agg_num* **[-***agg_num2***] accounting**

Syntax Definitions

agg_num	Specifies the aggregate group. Configured through the **static linkagg size** or **lacp linkagg size** command.
agg_num2	Last aggregate group in the range of linkagg.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Accounting information such as undersized and oversized packets received or transmitted, packets of a certain size, and Jabber frames is displayed.
- Accounting information shall be displayed for a single linkagg or range of linkagg.
- If no linkagg ID is specified, then the accounting information is displayed for all link aggregate IDs configured on the switch.

Examples

```
-> show linkagg 20 accounting
Linkagg = 20
  64 Octets          =              5509191,
  65   ~  127 Octets =                   44,
  128  ~  255 Octets =                   67,
  256  ~  511 Octets =                  174,
  512  ~ 1023 Octets =                 1964,
  1024 ~ MAX Octets =                  2715,
    RX:
      Undersize    =                19986,
      Oversize     =                 1771,
      Jabber       =                  368,
    TX:
      Undersize    =                    0,
      Oversize     =                    0,
```

output definitions

64 Octects	Number of transmitted and received frames that are 64 bytes in size.
65 ~ 127 Octets	Number of transmitted and received frames that are 65 to 127 bytes in size.

output definitions

128 ~ 255 Octets	Number of transmitted and received frames that are 128 to 255 bytes in size.
256 ~ 511 Octets	Number of transmitted and received frames that are 256 to 511 bytes in size.
512 ~ 1023 Octets	Number of transmitted and received frames that are 512 to 1023 bytes in size.
1024 ~ MAX Octets	Number of transmitted and received frames that are more than 1023 bytes in size and less than the size of MRU.
RX	
Undersize	Number of under size frame received.
Oversize	Number of over size frame received.
Jabber	Number of jabber frames received.
TX	
Undersize	Number of under size frame transmitted.
Oversize	Number of over size frame transmitted.

Release History

Release 6.7.2.R06; command introduced.

Related Commands

show linkagg counters	Displays the counter statistics such as such as unicast, multicast, broadcast frames transmitted and received by the ports in the linkagg.
show linkagg traffic	Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.
linkagg no l2-statistics	Clears statistics for all link aggregates or for specific aggregate IDs.

MIB Objects

```
alclnkaggAggIdAccountTable
   alcRxUndersize
   alcTxUndersize
   alcRxOversize
   alcTxOversize
   alcRxPackets64
   alcRxPackets127
   alcRxPackets255
   alcRxPackets511
   alcRxPackets1023
   alcRxPacketsMax
   alcRxJabberFrames
```

show linkagg counters

Displays the counter statistics such as such as unicast, multicast, broadcast frames transmitted and received by the ports in the linkagg.

show linkagg *agg_num* **[-***agg_num2***] counters [errors]**

Syntax Definitions

agg_num	Specifies the aggregate group. Configured through the **static linkagg size** or **lacp linkagg size** command.
agg_num2	Last aggregate group in the range of linkagg.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Statistics are displayed (in bytes or frame count) for all link aggregate IDs configured on the switch.
- This command will display the error packets statistics transmitted and received in the linkagg. Error statistics include the number of alignment, frame check (FCS), received, and transmitted errors.
- Counters information is be displayed for a single linkagg or for a range of linkagg.
- If no linkagg ID is specified, then counters value of all linkagg configured will be displayed.

Examples

```
-> show linkagg counters
Linkagg  1:
InOctets      =          54853143493,  OutOctets      =         627004300233,
InUcastPkts   =            106999474,  OutUcastPkts   =           1224280526,
InMcastPkts   =               302983,  OutMcastPkts   =               368866,
InBcastPkts   =               131517,  OutBcastPkts   =               430469,
InPauseFrames =                    0,  OutPauseFrames =                    0

Linkagg  2:
InOctets      =             41130472,  OutOctets      =             54807378,
InUcastPkts   =                  857,  OutUcastPkts   =                  857,
InMcastPkts   =               299227,  OutMcastPkts   =               368862,
InBcastPkts   =                    0,  OutBcastPkts   =                    0,
InPauseFrames =                    0,  OutPauseFrames =                    0

-> show linkagg 1 counters
Linkagg  1:
InOctets      =          54860911724,  OutOctets      =         627095472636,
InUcastPkts   =            107014627,  OutUcastPkts   =           1224458552,
InMcastPkts   =               303031,  OutMcastPkts   =               368920,
```

```
InBcastPkts   =              131533,  OutBcastPkts   =              430519,
InPauseFrames =                   0,  OutPauseFrames =                   0

-> show linkagg 1 counters errors
Link Agg 1
Alignments Errors       = 0
FCS Errors              = 0
IfInErrors              = 0
IfOutErrors             = 0
```

output definitions

InOctets	Number of octects received.
OutOctets	Number of octects transmitted.
InUcastPkts	Number of unicast frame received.
OutUcastPkts	Number of unicast frame transmitted.
InMcastPkts	Number of multicast frame received.
OutMcastPkts	Number of multicast frame transmitted.
InBcastPkts	Number of broadcast frame received.
OutBcastPkts	Number of broadcast frame transmitted.
InPauseFrames	Number of pause frame received.
OutPauseFrames	Number of pause frame transmitted.
Alignments Errors	Alignment error count.
FCS Errors	Frame check error count.
IfInErrors	Rx error count.
IfOutErrors	Tx error count.

Release History

Release 6.7.2.R06; command introduced.

Related Commands

show linkagg accounting	Displays statistics collected for packets transmitted and received on link aggregate ports.
show linkagg traffic	Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.
linkagg no l2-statistics	Clears statistics for all link aggregates or for specific aggregate IDs.

MIB Objects

```
alclnkaggAggIdCounterTable
   alcInOctets
   alcOutOctets
   alcInUcastPkts
   alcOutUcastPkts
   alcInMcastPkts
   alcOutMcastPkts
   alcInBcastPkts
   alcOutBcastPkts
```

```
   alcInPauseFrames
   alcOutPauseFrames
alclnkaggAggIdCounterErrTable
   alcAlignmentsErrors
   alcFCSErrors
   alcIfInErrors
   alcIfOutErrors
```

show linkagg traffic

Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.

show linkagg *agg_num* **[-***agg_num2***] traffic**

Syntax Definitions

agg_num	Specifies the aggregate group. Configured through the **static linkagg size** or **lacp linkagg size** command.
agg_num2	Last aggregate group in the range of linkagg.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Traffic information is displayed for a single linkagg as well as for range of linkagg.
- If no linkagg ID is specified, then the traffic information is displayed for all link aggregate IDs configured on the switch.

Examples

```
-> show linkagg traffic
              Input             Input              Output           Output
Agg           Packets           Bytes              Packets          Bytes
--------+-----------------+-----------------+----------------+--------------
1            107269377        54769099234         1223196904      626040576392
2            299624           41067322            369162          54725004
10           298373           38429849            587271          164105065
11           155992557        79653465622         86078418        43752546145
12           156611855        80126057543         9471314         4652930410

-> show linkagg 1 traffic
            Input             Input              Output             Output
Agg         Packets           Bytes              Packets            Bytes
--------+-----------------+---------------------------------+--------------
1           107396329        54833918534        1224653076       626785870115
```

output definitions

Agg	The link aggregate group.
Input Packets	Total packets received.
Input Bytes	Total bytes received.
Output Packets	Total packets transmitted.
Output Bytes	Total bytes transmitted.

Release History

Release 6.7.2.R06; command introduced.

Related Commands

show linkagg accounting	Displays statistics collected for packets transmitted and received on link aggregate ports.
show linkagg counters	Displays the counter statistics such as such as unicast, multicast, broadcast frames transmitted and received by the ports in the linkagg.
linkagg no l2-statistics	Clears statistics for all link aggregates or for specific aggregate IDs.

MIB Objects

```
alclnkaggAggIdTrafficTable
   alcInputPackets
   alcInputBytes
   alcOutputPackets
   alcOutputBytes
```

linkagg no l2-statistics

Clears statistics for all link aggregates or for a specific aggregate ID or range of IDs.

linkagg {all | *agg_num* **[-***agg_num2***]} no l2-statistics**

Syntax Definitions

*agg_id***[-***agg_id2***]**	The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command will reset accounting, counters, counters errors, traffic statistics to zero of all ports in the linkagg.
- If no linkagg ID is specified, then statistics are cleared for all link aggregates.
- Clearing interface statistics will not impact on link aggregation statistics, similarly clearing of link aggregation statistics will not impact interface statistics.

Examples

```
-> linkagg all no l2-statistics
-> linkagg 31 no l2-statistics
```

Release History

Release 6.7.2.R06; command introduced.

Related Commands

show linkagg accounting	Displays statistics collected for packets transmitted and received on link aggregate ports.
show linkagg counters	Displays statistics collected for the type and number of packets transmitted and received on link aggregate ports.
show linkagg traffic	Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.

MIB Objects

```
alcLagClearStats
```

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 6450, 6350

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 link A port and link B port to the session before administratively enabling the DHL session is allowed.

Examples

```
-> dhl num 1 name dhl_session1
-> no dhl num 1
```

Release History

Release 6.6.3; command 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/port	The slot number and the physical port number to designate as a link for the DHL session. (for example, 3/1 specifies port 1 on slot 3).
agg_id	The link aggregate ID number to designate as a link for the DHL session.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- Ensure that the 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 must 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 that 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.
- If the aggregate is configured as a link for a DHL session, you cannot remove a link aggregate from the switch configuration.

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 6.6.3; command 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 6450, 6350

Usage Guidelines

- The DHL session ID specified with this command must 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 6.6.3; command introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
dhl num linka linkb	Configures the two links required for a 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 6450, 6350

Usage Guidelines

- Create a DHL session prior to VLAN-MAP configuration.
- 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 having 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 is automatically 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 is also 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 6.6.3; command 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.
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 DHL 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 10 - 600.

Defaults

parameter	default
num	30 seconds

Platforms Supported

OmniSwitch 6450, 6350

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 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, configure mac-flush mechanism for faster convergence.

Examples

```
-> dhl num 1 pre-emption-time 40
```

Release History

Release 6.6.3; command 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 dual homed 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

Defaults

parameter	default
none | raw | mvrp	**none**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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 6.6.3; command 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 dual homed 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 6450, 6350

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 6.6.3; command 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 dual homed 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 6450, 6350

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. VLAN map 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 6.6.3; command introduced.

Related Commands

dhl num	Configures a session ID for the DHL session.
show dhl num link	Displays information about a specific dual homed 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 6450, 6350

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 6.6.3; command 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
   alaDHLVlanMapVlanStart
   alaDHLVlanMapVlanEnd
```

13 802.1AB Commands

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 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 security mechanism 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 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 dot3 power-via-mdi** **lldp tlv med** **lldp tlv proprietary** **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 6450, 6350

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
```

Release History

Release 6.6.2; 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 6450, 6350

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 6.6.2; 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.

lldp transmit interval *seconds*

Syntax Definitions

seconds	The transmit interval between LLDPDUs, in seconds. The valid range is 5 - 32768.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The LLDP protocol must be enabled before using this command.

Examples

```
-> lldp transmit interval 40
```

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

- The LLDP protocol must be enabled before using this command.
- The Time to Live is a multiple of transmit interval and transmit hold multiplier.

Examples

```
-> lldp transmit hold-multiplier 6
```

Release History

Release 6.6.1; command introduced.

Related Commands

lldp destination mac-address	Sets the transmit time interval for LLDPDUs. Time interval 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 time interval between successive LLDPDUs transmitted, in seconds. The valid range is 1-8192.

Defaults

parameter	default
seconds	2

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The LLDP protocol must be enabled before using this command.
- The transmit delay is less than or equal to the multiplication of transmit interval and 0.25 (transmit interval * 0.25).

Examples

```
-> lldp transmit delay 20
```

Release History

Release 6.6.1; command introduced.

Related Commands

lldp destination mac-address	Sets the transmit time interval for LLDPDUs. Time interval 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 time interval that must elapse before the status of a port is reinitialized after a status change.

lldp reinit delay *seconds*

Syntax Definitions

seconds	The number of seconds to reinitialize the ports status after a status change. The valid range is 1-10.

Defaults

parameter	default
seconds	2

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The LLDP protocol must be enabled before using this command.

Examples

```
-> lldp reinit delay 4
```

Release History

Release 6.6.1; command introduced.

Related Commands

lldp transmit delay	Sets the minimum time interval between successive LLDPDUs transmitted.
show lldp local -system	Displays local system information.

MIB Objects

```
lldpConfiguration
   lldpReinitDelay
```

lldp notification interval

Sets the time interval that must elapse before a notification about the local system MIB change is generated.

lldp notification interval *seconds*

Syntax Definitions

seconds	The minimum number of seconds for generating a notification-event. The valid range is 5-3600.

Defaults

parameter	default
seconds	5

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The LLDP protocol and notification must be enabled before using this command.
- In a specified interval, generating more than one notification-event is not possible.

Examples

```
-> lldp notification interval 25
```

Release History

Release 6.6.1; 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 switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

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 LLDPDUs transmission and reception.

Defaults

parameter	default
tx | rx | tx-and-rx | disable	**tx-and-rx**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The port can be set to receive, transmit, or transmit and receive LLDPDUs using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.

Examples

```
-> lldp 1/2 lldpdu tx-and-rx
-> lldp chassis lldpdu disable
```

Release History

Release 6.6.1; 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.
lldp tlv proprietary	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	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 6450, 6350

Usage Guidelines

- The LLDPDU administrative status must be in the receive state before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.

Examples

```
-> lldp 1/2 notification enable
-> lldp 1 notification disable
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.2; command introduced.

Related Commands

lldp tlv dot3 power-via-mdi	Configures whether 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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to disassociate a network policy from a port.
- The network policy must already be configured in the system before associating it with a port.
- A maximum of eight-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 6.6.2; command introduced.

Related Commands

lldp tlv dot3 power-via-mdi	Configures whether 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

Configures the switch to control per port management TLVs to be included 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 6450, 6350

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.

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 6.6.1; command introduced.

Related Commands

lldp lldpdu	Configures 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 per port information.
show lldp remote-system	Displays per local port and information of remote system.

MIB Objects

```
lldpPortConfigTable
   lldpLocPortPortNum
   lldpPortConfigTLVsTxEnable
lldpConfigManAddrTable
   lldpConfigManAddrPortsTxEnable
```

lldp tlv dot1

Configures the switch to control per port 802.1 TLVs to be included 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 6450, 6350

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- 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 6.6.1; command introduced.

Related Commands

lldp tlv management	Configures the switch to control per port management TLVs to be included 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 the switch to control per port 802.3 TLVs to be included in the 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.
enable	Enables 802.3 TLV LLDPDU transmission.
disable	Disables 802.3 TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.

Examples

```
-> lldp 2/4 tlv dot3 mac-phy enable
-> lldp 2 tlv dot3 mac-phy disable
```

Release History

Release 6.6.1; 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 the switch to control per port management TLVs to be included in the LLDPDUs.
lldp tlv dot1	Configures the switch to control per port 802.1 TLVs to be included in the LLDPDUs.
show lldp statistics	Displays per port statistics.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
lldpXdot3PortConfigTable
   lldpXdot3PortConfigTLVsTxEnable
```

lldp tlv dot3 power-via-mdi

Configures the switch to use the power via MDI TLV in the LLDPDU sent by the powered device.

lldp {*slot/port* **|** *slot* | **chassis} tlv dot3 power-via-mdi {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 chassis.
enable	Enables 802.3 TLV LLDPDU transmission.
disable	Disables 802.3 TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- When power-via-mdi is configured the power is negotiated between the powered device and the switch using the optional MDI TLV in the LLDPDU.

Examples

```
-> lldp 2/4 tlv dot3 power-via-mdi enable
-> lldp 2 tlv dot3 power-via-mdi disable
```

Release History

Release 6.6.5; 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 the switch to control per port management TLVs to be included in the LLDPDUs.
lldp tlv dot1	Configures the switch to control per port 802.1 TLVs to be included in the LLDPDUs.
show lldp statistics	Displays per port statistics.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
lldpXdot3PortConfigTable
   lldpXdot3PortConfigTLVsTxEnable
```

lldp tlv med

Configures the switch to control per port LLDP-MED (Media Endpoint Device) TLVs to be included in the 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	Enables or disables transmission of LLDP-MED capabilities TLV in LLDPDU.
network policy	Includes the network policy TLV in transmitted LLDPDUs.
enable	Enables LLDP-MED TLV LLDPDU transmission.
disable	Disables LLDP-MED TLV LLDPDU transmission.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- 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 6.6.1; command introduced.
Release 6.6.2; **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 the switch to control per port management TLVs to be included in the LLDPDUs.
lldp tlv dot1	Configures the switch to control per port 802.1 TLVs to be included in the LLDPDUs.
lldp tlv dot3 mac-phy	Configures the switch to control per port 802.3 TLVs to be included in the LLDPDUs.
show lldp med network-policy	Displays the MED Network Policy configuration.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
lldpXMedPortConfigTable
   lldpXMedPortConfigTLVsTxEnable
```

lldp tlv proprietary

Allows the switch to advertise the Access Point location through the proprietary TLVs.

lldp {*slot/port* **|** *slot* | **chassis} tlv proprietary {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 switch ports.
enable	Enables proprietary TLVs to advertise AP location.
disable	Disables proprietary TLVs to advertise AP location.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The VLAN information is advertised through 802.1x TLV (i.e, Management VLAN is advertised if the port is a 802.1x port else default VLAN of the port is advertised). The AP location is advertised through proprietary TLV.
- If an AP is detected and authenticated on a 802.1x port, LLDP TLVs are triggered to advertise management VLAN and AP location despite CLI configuration being disabled.
- If an AP is removed from 802.1x port, LLDP receives message from 802.1x port after which LLDP stops advertising of management VLAN and AP location, only if the configuration is disabled explicitly on the port.

Examples

```
-> lldp 5/1 tlv proprietary enable
-> lldp 5/1 tlv proprietary disable
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

lldp tlv management	Configures the switch to control per port management TLVs to be included in the LLDPDUs.
show lldp statistics	Displays per port statistics.
show lldp local -port	Displays per port information.

MIB Objects

```
alaLldpPropConfigTable
   alaLldpPropAPLocation
```

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 6450, 6350

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  | Proprietary
 Slot/Port| Status |  Trap   |   Mask  | Address |  TLV    |  Mask   |  Mask  |    TLV
----------+--------+---------+---------+---------+---------+---------+--------+-------------------
   3/1    Rx + Tx  Disabled   0x00     Disabled  Disabled   0x00      0x00     Disabled
   3/2    Rx + Tx  Disabled   0x00     Disabled  Disabled   0x00      0x00     Disabled
   3/3    Rx + Tx  Disabled   0x00     Disabled  Disabled   0x00      0x00     Disabled
   3/4    Rx + Tx  Disabled   0xa0     Disabled  Enabled    0x00      0x00     Disabled
   3/5    Rx + Tx  Disabled   0x00     Disabled  Disabled   0x00      0x00     Disabled
   3/6    Rx + Tx  Disabled   0x00     Disabled  Disabled   0x00      0x00     Disabled
```

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 whether 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.

output definitions

802.1 TLV	Indicates whether 802.1 TLV status is enabled or disabled on the LLDP port.
802.3 Mask	The standard 802.3 mask set for the port.
MED Mask	The standard MED mask set for the port.
Proprietary TLV	Indicates the proprietary TLV status.

Release History

Release 6.6.1; command introduced.
Release 6.7.2.R02; **Proprietary TLV** output field included.

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	Configures the switch to control per port management TLVs to be included in the LLDPDUs.
lldp tlv dot3 mac-phy	Configures the switch to control per port 802.3 TLVs to be included in the LLDPDUs.
lldp tlv proprietary	Allows the switch to advertise the Access Point location through the proprietary TLVs.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
   lldpPortConfigAdminStatus
   lldpPortConfigNotificationEnable
   lldpLocPortPortNum
   lldpPortConfigTLVsTxEnable
lldpConfigManAddrTable
   lldpConfigManAddrPortsTxEnable
lldpXdot3PortConfigTable
   lldpXdot3PortConfigTLVsTxEnable
alaLldpPropConfigTable
   alaLldpPropAPLocation
```

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 6450, 6350

Usage Guidelines

- Network policy must 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 6.6.2; 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 6450, 6350

Usage Guidelines

- Network policy must 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 6.6.2; command introduced.

Related Commands

lldp tlv dot3 power-via-mdi	Configures whether 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 6450, 6350

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 6.6.1; 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/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, statistics are displayed for all LLDP ports.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 the switch to control per port management TLVs to be included 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 6450, 6350

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                 = vxTarget,
  System Description          = Alcatel-Lucent 6450 10 PORT COPPER GE 6.6.3.177.
                                R01 Development, February 10, 2012.,
  Capabilities Supported      = Bridge, Router,
  Capabilities Enabled        = Bridge, Router,
  LLDPDU Transmit Interval    = 30 seconds,
  TTL Hold Multiplier         = 4,
  LLDPDU Transmit Delay       = 2 seconds,
  Reinitialization Delay      = 2 seconds,
  MIB Notification Interval   = 5 seconds
  Fast Start Count            = 3,
  Management Address Type     = 1 (IPv4),
  Management IP Address       = 10.255.13.44,
```

output definitions

Chassis ID Subtype	The subtype that specifies the 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.

output definitions (continued)

TTL Hold Multiplier	The hold multiplier used to calculate TTL.
LLDPDU Transmit Delay	The minimum transmit time between successive LLDPDUs.
Reinitialization 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	Configures 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. The Loopback0 IP address (if configured) is considered as the management IP address, else, the first IP interface configured on the switch is considered.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; **Fast Start Count** field added to output.

Related Commands

lldp destination mac-address	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 per 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show lldp local-port
Local Slot 1/Port 1 LLDP Info:
  Port ID                     = 1001 (Locally assigned),
  Port Description            = Alcatel-Lucent 1/1,
  Vlan                        = 1,
  AP Location                 = sw1,
Local Slot 1/Port 2 LLDP Info:
  Port ID                     = 1002 (Locally assigned),
  Port Description            = Alcatel-Lucent 1/2,
  Vlan                        = 1,
  AP Location                 = -,
Local Slot 1/Port 3 LLDP Info:
  Port ID                     = 1003 (Locally assigned),
  Port Description            = Alcatel-Lucent 1/3,
  Vlan                        = 1,
  AP Location                 = -,
Local Slot 1/Port 4 LLDP Info:
  Port ID                     = 1004 (Locally assigned),
  Port Description            = Alcatel-Lucent 1/4,
  Vlan                        = 1,
  AP Location                 = -,
Local Slot 1/Port 5 LLDP Info:
  Port ID                     = 1005 (Locally assigned),
  Port Description            = Alcatel-Lucent 1/5,
  Vlan                        = 1,
  AP Location                 = -,
Local Slot 1/Port 6 LLDP Info:
  Port ID                     = 1006 (Locally assigned),
```

```
  Port Description           = Alcatel-Lucent 1/6,
  Vlan                       = 4095,
  AP Location                = -,
Local Slot 1/Port 7 LLDP Info:
  Port ID                    = 1007 (Locally assigned),
  Port Description           = Alcatel-Lucent 1/7,
  Vlan                       = 1,
  AP Location                = -,
Local Slot 1/Port 8 LLDP Info:
  Port ID                    = 1008 (Locally assigned),
  Port Description           = Alcatel-Lucent 1/8,
  Vlan                       = 4003,
  AP Location                = -,
Local Slot 1/Port 9 LLDP Info:
  Port ID                    = 1009 (Locally assigned),
  Port Description           = Alcatel-Lucent 1/9,
  Vlan                       = 4095,
  AP Location                = -,
Local Slot 1/Port 10 LLDP Info:
  Port ID                    = 1010 (Locally assigned),
  Port Description           = Alcatel-Lucent 1/10,
  Vlan                       = 4095,
  AP Location                = -
```

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).
Vlan	Displays the authenticated VLAN (management VLAN) if AP is connected on a dot1x enabled port, else the default VLAN of the port is displayed.
AP Location	Displays the location to which the AP is connected.

Release History

Release 6.6.1; command introduced.
Release 6.7.2.R02; **Vlan** and **AP Location** output fields included.

Related Commands

lldp tlv management	Configures the switch to control per port management TLVs to be included in the LLDPDUs.
lldp tlv dot1	Configures the switch to control per port 802.1 TLVs to be included in the LLDPDUs.
lldp tlv proprietary	Allows the switch to advertise the WLAN VLAN information and Access Point location through the proprietary TLVs.

MIB Objects

```
lldpLocPortTable
   lldpLocPortNum
   lldpLocPortIdsubtype
   lldpLocPortId
```

```
lldpLocPortDesc
alaLldpPropAPLocation
alaLldpPropVlan
alaLldpPropLocationDesc
```

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 6450, 6350

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 6.6.1; command introduced.

Related Commands

lldp tlv management	Configures the switch to control per port management TLVs to be included in the LLDPDUs.
show lldp local -system	Displays local system information.

MIB Objects

```
lldpLocManAddrTable
   lldpLocManAddrLen
   lldpLocManAddrIfSubtype
   lldpLocManAddrIfId
```

show lldp remote-system

Displays per local port and information of remote system.

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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show lldp remote-system
Remote LLDP Agents on Local Slot/Port: 2/47,
  Chassis ID Subtype          = 4 (MAC Address),
  Chassis ID                  = 00:d0:95:e9:c9:2e,
  Port ID Subtype             = 7 (Locally assigned),
  Port ID                     = 2048,
  Port Description            = (null),
  System Name                 = (null),
  System Description          = (null),
  Capabilities Supported       = none supported,
  Capabilities Enabled         = none enabled,

Remote LLDP Agents on Local Slot/Port: 2/48,
  Chassis ID Subtype          = 4 (MAC Address),
  Chassis ID                  = 00:d0:95:e9:c9:2e,
  Port ID Subtype             = 7 (Locally assigned),
  Port ID                     = 2047,
  Port Description            = (null),
  System Name                 = (null),
  System Description          = (null),
  Capabilities Supported       = none supported,
  Capabilities Enabled         = none enabled,
```

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 specifies the chassis ID.
Chassis ID	The chassis ID (MAC address).
Port ID Subtype	The sub type that specifies the port ID.
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.
Capabilities Enabled	The enabled capabilities of the system.

Release History

Release 6.6.1; command 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 6450, 6350

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 2/47 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 2/47 remote-system med inventory
Remote LLDP Agents on Local Slot/Port 1/22:
  Remote ID  1:
    MED Hardware Revision = "1.2.12.3",
    MED Firmware Revision = "6.3.4.1",
    MED Software Revision = "4.2.1.11",
    MED Serial Number        = "32421",
    MED Manufacturer Name = "Manufacturer1",
    MED Model Name = "Alc32d21",
    MED Asset ID = "124421",
  Remote ID  2:
    MED Hardware Revision = "1.2.12.4",
    MED Firmware Revision = "6.3.4.2",
    MED Software Revision = "4.2.1.13",
    MED Serial Number        = "32424",
    MED Manufacturer Name = "Manufacturer2",
    MED Model Name = "Alc32d41",
     MED Asset ID = "124424",
```

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 6.6.1; 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}**

lldp {*slot/port***|** *slot* **| chassis} [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 6450, 6350

Usage Guidelines

- By enabling security on chassis or slot level, the ports that come under the respective levels 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 an LLDP security enabled port, LLDP CMM waits for three times the LLDP timer interval (30 seconds). If LLDP PDU is not received after link up that has no remote agent, the port is moved to a violation state.
- If a trusted remote agent exists, and if no LLDP remote agent is learned even after three times the LLDP timer interval (30 seconds), the port is moved to 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 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 6.6.3; 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/port.

MIB Objects

```
alaLldpTrustAdminStatus
   alaLldpTrustChassiIdSubType
```

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 6450, 6350

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 comes up. The port 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 6.6.3; 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/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 6450, 6350

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 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 specifies the chassis ID.
Chassis ID	The chassis ID (MAC address).
Port ID Subtype	The sub type that specifies port ID.
Port ID	The port ID (Port MAC).

Release History

Release 6.6.3; 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/port.

show lldp [*num* **|** *slot/port***] trust-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 6450, 6350

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 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     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/5     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/6     Enabled        Trap Only         Trusted            1(Chassis Component)
   1/7     Enabled        Trap Only         Trusted            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)
   1/11    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/12    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/13    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/14    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/15    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/16    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/17    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/18    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/19    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/20    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/21    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/22    Enabled        Trap Only         Trusted            1(Chassis Component)
   1/23    Enabled        Trap Only         Trusted            1(Chassis Component)
```

```
1/24    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 specifies the chassis ID.

Release History

Release 6.6.3; 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
```

14 Interswitch Protocol Commands

Alcatel Interswitch Protocols (AIP) are used to discover and advertise adjacent switch information. Only one protocol is supported:

Alcatel Mapping Adjacency Protocol (AMAP), used to discover the topology of OmniSwitches.

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 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 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

- Use of the **time** command keyword is optional.
- When AMAP is enabled, all active Spanning Tree ports start out in the discovery transmission state.
- Ports that receive Hello packets before three discovery transmission times expire, send a Hello reply and transition to the common transmission state.
- Ports that do not receive Hello packets before three discovery transmission times expire, revert to the passive reception state.
- Ports in the passive reception state do not send Hello packets and do not use any timer to determine how long to wait for Hello packets.
- The discovery transmission time value is also used by ports in the common transmission state to determine how long to wait for Hello packets (see page 14-5).

Examples

```
-> amap discovery 1200
-> amap discovery time 600
```

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

- Use of the **time** command keyword is optional.
- To avoid synchronization with adjacent switches, the common transmission time is jittered randomly by plus or minus ten percent. For example, if the default time is used (300 seconds), the jitter is plus or minus 30 seconds.
- The common transmission time value is only used by ports in the common transmission state.
- If a Hello packet is received from an adjacent switch before the common transmission time has expired, the switch sends a Hello reply and restarts the common transmission timer.
- A port reverts to the discovery transmission state if a Hello response is not received after the discovery time interval (see page 14-3) has expired.

Examples

```
-> amap common 1200
-> amap common time 600
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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.

MIB Objects

N/A

15 802.1Q Commands

Alcatel's 802.1Q is an IEEE standard for sending frames through the network tagged with VLAN identification. This chapter details configuring and monitoring 802.1Q tagging on a single port in a switch or an aggregate of ports on a switch.

Alcatel's version of 802.1Q complies with the Draft Standard *P802.1Q/D11 IEEE Standards for Local And Metropolitan Area Network: Virtual Bridged Local Area Networks, July 30, 1998.*

MIB information for the 802.1Q commands is as follows:

Filename: alcatelIND1Dot1Q.mib
Module: ALCATEL-IND1-DOT1Q-MIB

A summary of available commands is listed here:

vlan 802.1q
vlan 802.1q frame type
show 802.1q

Note. Before using 802.1Q, the VLAN for 802.1Q must be created using the commands described in Chapter 25, "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 handles 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 (for example, “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 6450, 6350

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 25, “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 12, “Link Aggregation Commands” for more information on link aggregation.
- The port’s default VLAN can never be configured to accepted tagged frames.
- This command is also supported on an NNI interface.
- An error message is displayed, if the TPID of the NNI port is other than 0x8100 while configuring the port as 802.1Q tagged. An error message is displayed, if the user tries to configure TPID, other than 0x8100, on 802.1Q tagged NNI interface.
- An error message is displayed, if VLAN 1 is tried to be configured as default VLAN on an NNI port.

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 6.6.1; command was introduced.
Release 6.6.5; command supported on NNI interface.

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 6450, 6350

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 (that is, untagged frames or priority-tagged frames) is 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 6.6.1; 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 12, "Link Aggregation Commands" for more information on link aggregation.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show 802.1q 3/4

  Acceptable Frame Type   :      Any Frame Type
  Force Tag Internal      :                 off

  Tagged VLANS      Internal Description
  ------------+-------------------------------------------------+
              2      TAG PORT 3/4 VLAN 2


  -> show 802.1q 2

  Tagged VLANS      Internal Description
  ------------+-------------------------------------------------+
              3      TAG AGGREGATE 2 VLAN 3
```

Output fields are described here:

output definitions

Acceptable Frame Type	The acceptable frame type for this port, which can be **Any Frame Type** or **Tagged Only Frame Type**.
Force Tag Internal	This field displays if adding the default VLAN ID (VID) to tagged frames is turned **on** or **off**.

output definitions (continued)

Tagged VLANS	The 802.1Q tag number for this port.
Internal Description	The description of this 802.1Q tag. You can modify this description with the **vlan 802.1q** command, which is described on page 15-2.

Release History

Release 6.6.1; 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
```

16 Distributed Spanning Tree Commands

The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the Alcatel STP implementation distributes the Spanning Tree load between the primary management module and the network interface modules. In the case of a stack of switches, the STP load is distributed between the primary management switch and other switches in the stack. This functionality improves network robustness by providing a Spanning Tree that continues to respond to BPDUs and port link up and down states in the event of a fail over to a backup management module or switch.

In addition to a distributed architecture, this implementation also provides the following Spanning Tree features:

- Automatic configuration of a physical topology into a single Spanning Tree to ensure that there is only one data path between any two switches.
- Fault tolerance within the network topology. The Spanning Tree is reconfigured in the event of a data path or bridge failure or when a new switch is added to the topology.
- Support for 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 up to 16 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 128 rings 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 hello time** **bridge max age** **bridge forward delay** **bridge bpdu-switching** **bridge path cost mode** **bridge auto-vlan-containment** **show spantree** **show spantree mode**
Explicit bridge commands	**bridge cist protocol** **bridge 1x1 protocol** **bridge cist priority** **bridge msti priority** **bridge 1x1 priority** **bridge cist hello time** **bridge 1x1 hello time** **bridge cist max age** **bridge 1x1 max age** **bridge cist forward delay** **bridge 1x1 forward delay** **show spantree cist** **show spantree msti** **show spantree 1x1**
Implicit port commands	**bridge slot/port** **bridge slot/port priority** **bridge slot/port path cost** **bridge slot/port mode** **bridge slot/port connection** **show spantree ports**

Explicit port commands	**bridge cist slot/port** **bridge 1x1 slot/port** **bridge cist slot/port priority** **bridge msti slot/port priority** **bridge 1x1 slot/port priority** **bridge cist slot/port path cost** **bridge msti slot/port path cost** **bridge 1x1 slot/port path cost** **bridge cist slot/port mode** **bridge 1x1 slot/port mode** **bridge cist slot/port connection** **bridge 1x1 slot/port connection** **bridge cist slot/port admin-edge** **bridge 1x1 slot/port admin-edge** **bridge cist slot/port auto-edge** **bridge 1x1 slot/port auto-edge** **bridge cist slot/port restricted-role** **bridge 1x1 slot/port restricted-role** **bridge cist slot/port restricted-tcn** **bridge 1x1 slot/port 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 mode 1x1 pvst+** **bridge port 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 6450, 6350

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 will block 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 in that it will have its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max age, and forward delay.
- When operating in 1x1 mode, 802.1Q tagged ports participate in an 802.1Q Spanning Tree instance that allows the Spanning Tree to extend across tagged VLANs. As a result, a tagged port may participate in more than one Spanning Tree instance; one for each VLAN that the port carries.
- If a VLAN contains both fixed and tagged ports and the switch is operating in 1x1 Spanning Tree mode, then a hybrid of the two Spanning Tree instances (single and 802.1Q) is applied. If a VLAN appears as a tag on a port, then the BPDU for that VLAN are also tagged. However, if a VLAN appears as the configured default VLAN for the port, then BPDU are not tagged and the single Spanning Tree instance applies.
- Regardless of which mode the switch is running in, it is possible to administratively disable the Spanning Tree status for an individual VLAN (see Chapter 25, “VLAN Management Commands”). Note that active ports associated with such a VLAN are excluded from any Spanning Tree calculations and will remain in a forwarding state.

Examples

```
-> bridge mode flat
-> bridge mode 1x1
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge protocol	Selects the Spanning Tree protocol for the specified instance.
bridge bpdu-switching	Enables the switching of Spanning Tree BPDU on a VLAN that has Spanning Tree disabled.
show spantree	Displays VLAN Spanning Tree parameter values.

MIB Objects

```
vStpTable
   vStpNumber
   vStpMode
```

bridge protocol

Configures the Spanning Tree protocol for the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance if the switch is running in the 1x1 mode.

bridge [*instance***] protocol {stp | rstp | mstp}**

Syntax Definitions

instance	The flat mode CIST instance (1) or an existing 1x1 mode VLAN ID instance number (bridge 1–4094).
stp	IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
rstp	IEEE 802.1W Rapid Spanning Tree Protocol.
mstp	IEEE 802.1Q 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 6450, 6350

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.
- Note that 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.
- Deleting all existing MSTIs is required before changing the protocol from MSTP to STP or RSTP.

- Note that when changing the protocol to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values. However, if the path cost mode was set to 32-bit prior to the protocol change, the path cost is *not* reset to its default value. See the **bridge path cost mode** command page for more information.

Examples

```
-> bridge mode flat
-> bridge protocol mstp
-> bridge protocol rstp
-> bridge protocol stp

-> bridge mode 1x1
-> bridge 10 protocol rstp
-> bridge 200 protocol stp
-> bridge protocol mstp
-> bridge protocol rstp
-> bridge protocol stp
```

Release History

Release 6.6.1; command was introduced.

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 6450, 6350

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.
- Note that 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.
- Note that when changing the protocol to/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.
- If the switch is running in 1x1 mode when this command is used, the specified protocol is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.

Examples

```
-> bridge cist protocol rstp
-> bridge cist protocol mstp
-> bridge cist protocol stp
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge protocol	Implicit command for changing the Spanning Tree protocol for the flat mode instance or for a 1x1 mode VLAN instance.
bridge 1x1 protocol	Explicit command for changing the Spanning Tree protocol for a VLAN instance.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsProtocolSpecification
```

bridge 1x1 protocol

Configures the Spanning Tree protocol for an individual VLAN instance.

bridge 1x1 *vid* **protocol {stp | rstp}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
stp	IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
rstp	IEEE 802.1w Rapid Spanning Tree Protocol.

Defaults

RSTP is the default protocol for the flat mode CIST instance and for the 1x1 mode VLAN instance.

Platforms Supported

OmniSwitch 6450, 6350

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 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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge protocol	Implicit command for changing the Spanning Tree protocol for the flat mode instance or for a 1x1 mode VLAN instance.
bridge cist protocol	Explicit command for changing the Spanning Tree protocol for the flat mode instance.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsProtocolSpecification
```

bridge mst region name

Defines the name for a Multiple Spanning Tree (MST) region. One of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 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 (e.g. “Alcatel Marketing”).

Defaults

By default, the MST region name is left blank.

Platforms Supported

OmniSwitch 6450, 6350

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 Marketing”
-> bridge mst region no name
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge mst region revision level	Defines the revision level for an MST region.
bridge mst region max hops	Defines the maximum number of hops for the MST region.
bridge msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
bridge msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigName
```

bridge mst region revision level

Defines the revision level for a Multiple Spanning Tree (MST) region. One of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mst region name	Defines the name for an MST region.
bridge mst region max hops	Defines the maximum number of hops for the MST region.
bridge msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
bridge msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigRevisionLevel
```

bridge mst region max hops

Configures the maximum number of hops that are authorized to receive Multiple Spanning Tree (MST) regional information. Use this command to designate how many hops a BPDU is allowed to traverse before it is discarded and related information is aged.

bridge mst region max hops *max_hops*

Syntax Definitions

max_hops	A numeric value (1–40) that designates the maximum number of hops.

Defaults

By default, the maximum number of hops is set to 20.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mst region name	Defines the name for an MST region.
bridge mst region revision level	Defines the revision level for an MST region.
bridge msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
bridge msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionMaxHops
```

bridge msti

Defines a Multiple Spanning Tree Instance (MSTI) number. This number identifies an association between a range of VLANs and a single Spanning Tree instance. In addition, it is possible to assign an optional name to the MSTI for further identification.

bridge msti *msti_id* **[name** *name***]**

bridge no msti *msti_id*

bridge msti *msti_id* **no name**

Syntax Definitions

msti_id	A numeric value (1–4094) that uniquely identifies an MSTI.
name	An alphanumeric string up to 32 characters. Use quotes around string if the name contains multiple words with spaces between them (e.g. “Alcatel Marketing”).

Defaults

By default, a flat mode Common and Internal Spanning Tree (CIST) instance always exists. The MSTI ID number for this instance is 0.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mst region name	Defines the name for an MST region.
bridge mst region revision level	Defines the revision level for an MST region.
bridge mst region max hops	Defines the maximum number of hops for the MST region.
bridge msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapAddition
   vStpMstInstanceVlanBitmapDeletion
   vStpMstInstanceVlanBitmapState
```

bridge msti vlan

Defines an association between a range of VLANs and a single Multiple Spanning Tree Instance (MSTI). The MSTI-to-VLAN mapping created with this command is one of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 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 (e.g. 100-115 122 135 200-210).

Defaults

By default, all VLANs are associated with the flat mode Common and Internal Spanning Tree (CIST) instance, which is also known as MSTI 0.

Platforms Supported

OmniSwitch 6450, 6350

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. The MSTI configuration, however, is not active unless the switch is running in the flat mode.

Examples

```
-> bridge msti 10 vlan 100-115
-> bridge msti 20 vlan 122 135 200-210
-> bridge msti 10 no vlan 112 200-204
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge mst region name	Defines the name for an MST region.
bridge mst region revision level	Defines the revision level for an MST region.
bridge mst region max hops	Defines the maximum number of hops for the MST region.
bridge msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.

MIB Objects

```
vStpMstVlanAssignmentTable
   vStpMstVlanAssignmentVlanNumber
   vStpMstVlanAssignmentMstiNumber
```

bridge priority

Configures the bridge priority value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a 1x1 mode VLAN instance. Bridge priority is used to determine which bridge the Spanning Tree algorithm designates as the root bridge.

bridge [*instance***] priority** *priority*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
priority	A bridge priority value within the range of 0–65535. Do not use commas in the value. If MSTP is the active protocol on the switch, then a bridge priority value that is a multiple of 4096 is required.

Defaults

By default, the bridge priority value is set to 32768.

parameter	default
instance	flat mode instance

Platforms Supported

OmniSwitch 6450, 6350

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/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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist priority	Explicit command for changing the Spanning Tree priority for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge msti priority	Explicit command for changing the Spanning Tree priority for an 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 6450, 6350

Usage Guidelines

- The bridge priority specifies the priority value for the first two octets of the Bridge ID (eight octets long). The remaining six octets of the Bridge ID contain a dedicated bridge MAC address.
- The lower the bridge priority number, the higher the priority that is associated with the bridge.
- This command is an explicit Spanning Tree command that only applies to the CIST instance regardless of which operating mode (flat or 1x1) or protocol is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified priority value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when the protocol is changed to/from MSTP, 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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge priority	Implicit command for changing the Spanning Tree priority for the flat mode CIST instance or a 1x1 mode VLAN instance.
bridge msti priority	Explicit command for changing the Spanning Tree priority for an 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 6450, 6350

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/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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects a flat Spanning Tree or 1x1 (per VLAN) Spanning Tree operating mode for the switch.
bridge priority	Implicit command for changing the Spanning Tree priority for the flat mode CIST instance or a 1x1 mode VLAN instance.
bridge cist priority	Explicit command for changing the Spanning Tree priority for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 priority	Explicit command for changing the Spanning Tree priority for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsMstiNumber
   vStpInsMode
   vStpInsPriority
   vStpInsBridgeAddress
```

bridge 1x1 priority

Configures the bridge priority value for an individual VLAN instance.

bridge 1x1 *vid* **priority** *priority*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
priority	A bridge priority value within the range of 0–65535. Do not use commas in the value.

Defaults

By default, the bridge priority value is set to 32768.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects a flat Spanning Tree or 1x1 (per VLAN) Spanning Tree operating mode for the switch.
bridge priority	Implicit command for changing the Spanning Tree priority for the flat mode CIST instance or a 1x1 mode VLAN instance.
bridge cist priority	Explicit command for changing the Spanning Tree priority for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge msti priority	Explicit command for changing the Spanning Tree priority for an 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist hello time	Explicit command for changing the Spanning Tree hello time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 hello time	Explicit command for changing the Spanning Tree hello time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsBridgeHelloTime
```

bridge cist hello time

Configures the bridge hello time value for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the amount of time, in seconds, between each transmission of a BPDU on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root.

bridge cist hello time *seconds*

Syntax Definitions

seconds	Hello time value in seconds (1–10).

Defaults

By default, the bridge hello time value is set to 2 seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge hello time	Implicit command for changing the Spanning Tree hello time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge 1x1 hello time	Explicit command for changing the Spanning Tree hello time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsBridgeHelloTime
```

bridge 1x1 hello time

Configures the bridge hello time value for an individual VLAN instance. This value is the amount of time, in seconds, between each transmission of a BPDU on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root.

bridge 1x1 *vid* **hello time** *seconds*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
seconds	Hello time value in seconds (1–10).

Defaults

By default, the bridge Hello Time value is set to 2 seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge hello time	Implicit command for changing the Spanning Tree hello time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge cist hello time	Explicit command for changing the Spanning Tree hello time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsBridgeHelloTime
```

bridge max age

Configures the Spanning Tree bridge max age time for the flat mode Common and Internal Spanning Tree (CIST) instance or for a 1x1 mode VLAN instance. This value is the amount of time, in seconds, that Spanning Tree information learned from the network on any port is retained. When this information has aged beyond the max age value, the information is discarded.

bridge [*instance***] max age** *seconds*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
seconds	Max age time in seconds (6–40).

Defaults

By default, the bridge max age time value is set to 20 seconds.

parameter	default
instance	flat mode instance

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist max age	Explicit command for changing the Spanning Tree max age time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 max age	Explicit command for changing the Spanning Tree max age time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsBridgeMaxAge
```

bridge cist max age

Configures the bridge max age time value for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the amount of time, in seconds, that Spanning Tree Protocol information learned from the network on any port is retained. When this information has aged beyond the max age value, the information is discarded.

bridge cist max age *seconds*

Syntax Definitions

seconds	Max age time in seconds (6–40).

Defaults

By default, the bridge max age time value is set to 20 seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge max age	Implicit command for changing the Spanning Tree max age time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge 1x1 max age	Explicit command for changing the Spanning Tree max age time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsBridgeMaxAge
```

bridge 1x1 max age

Configures the bridge max age time value for an individual VLAN instance. This value is the amount of time, in seconds, that Spanning Tree Protocol information learned from the network on any port is retained. When this information has aged beyond the max age value, the information is discarded.

bridge 1x1 *vid* **max age** *seconds*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
seconds	Max age time in seconds (6–40).

Defaults

By default, the bridge max age time value is set to 20 seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge max age	Implicit command for changing the Spanning Tree max age time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge cist max age	Explicit command for changing the Spanning Tree max age time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsBridgeMaxAge
```

bridge forward delay

Configures the bridge forward delay time for the flat mode Common and Internal Spanning Tree (CIST) instance or for 1x1 mode VLAN instance. This value is the amount of time, in seconds, that determines how fast a port changes its Spanning Tree state until it reaches a forwarding state. The forward delay time specifies how long a port stays in the listening and learning states, which precede the forwarding state.

bridge [*instance***] forward delay** *seconds*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
seconds	Forward delay time, in seconds (4–30).

Defaults

By default, the bridge forward delay time value is set to 15 seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist forward delay	Explicit command for changing the Spanning Tree forward delay time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.
bridge 1x1 forward delay	Explicit command for changing the Spanning Tree forward delay time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.
bridge rrstp ring vlan-tag	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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge forward delay	Implicit command for changing the Spanning Tree forward delay time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge 1x1 forward delay	Explicit command for changing the Spanning Tree forward delay time value for a VLAN instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsBridgeForwardDelay
```

bridge 1x1 forward delay

Configures the bridge forward delay time value for an individual VLAN instance. This value is the amount of time, in seconds, that determines how fast a port changes its Spanning Tree state until it reaches a forwarding state. The forward delay time specifies how long a port stays in the listening and learning states, which precede the forwarding state.

bridge 1x1 *vid* **forward delay** *seconds*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
seconds	Forward delay time in seconds (4–30).

Defaults

By default, the bridge forward delay time value is set to 15 seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge forward delay	Implicit command for changing the Spanning Tree forward delay time value for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge cist forward delay	Explicit command for changing the Spanning Tree forward delay time value for the CIST instance when the switch is operating in either the flat or 1x1 mode.

MIB Objects

```
vStpInsTable
   vStpIns1x1VlanNumber
   vStpInsMode
   vStpInsBridgeForwardDelay
```

bridge bpdu-switching

Enables the switching of Spanning Tree BPDU on the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance if the switch is running in the 1x1 mode.

bridge [*instance***] bpdu-switching {enable | disable}**

Syntax Definitions

instance	The flat mode CIST instance (bridge 1) or an existing 1x1 mode VLAN ID instance number (bridge 1–4094).
enable	Enables BPDU switching for the specified instance.
disable	Disables BPDU switching for the specified instance.

Defaults

By default, BPDU switching is disabled for an instance.

parameter	default
instance	CIST (flat mode)

Platforms Supported

OmniSwitch 6450, 6350

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* will return an error message. BPDU switching is only configured for the flat mode instance (bridge 1), regardless of which protocol is active (STP, RSTP, or MSTP).

Examples

```
-> bridge mode flat
-> bridge bpdu-switching enable
-> bridge 1 bpdu-switching disable

-> bridge mode 1x1
-> bridge 100 bpdu-switching enable
-> bridge 100 bpdu-switching disable
```

Release History

Release 6.6.1; command was 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 6450, 6350

Usage Guidelines

- Note that all path cost values, except those for MSTIs, are reset to the default path cost value when this mode is changed.
- When connecting a switch running in the 32-bit path cost mode to a switch running in the 16-bit mode, the 32-bit switch will have a higher path cost value and thus an inferior path cost to the 16-bit switch. To avoid this, use the **bridge path cost mode** command to change the 32-bit switch to a 16-bit switch.
- Note that when the protocol is changed to/from MSTP, 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 6.6.1; command was introduced.

Related Commands

bridge slot/port path cost	Defines a Spanning Tree path cost for a port.
bridge protocol	Configures the protocol for the flat mode CIST instance or a 1x1 mode VLAN instance.

MIB Objects

```
vStpBridge
   vStpPathCostMode
```

bridge 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge slot/port 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 slot/port

Enables or disables the Spanning Tree status on a single port or an aggregate of ports for the specified flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance.

bridge *instance* **{***slot/port* **|** *logical_port***} {enable | disable}**

Syntax Definitions

instance	The CIST instance number or an existing VLAN ID number (1–4094).
slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	The Link aggregate ID number (0–31).
enable	Enables Spanning Tree on the specified port for the specified instance.
disable	Disables Spanning Tree on the specified port for the specified instance.

Defaults

By default, the Spanning Tree status is enabled on eligible ports.

Platforms Supported

OmniSwitch 6450, 6350

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 slot/port** 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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port	Explicit command for configuring the Spanning Tree status on a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port	Explicit command for configuring the Spanning Tree status on a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.
vlan stp	Enables or disables the Spanning Tree instance for a VLAN.
bridge bpdu-switching	Enables or disables BPDU switching for the specified VLAN.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortEnable
```

bridge cist slot/port

Enables or disables the Spanning Tree status on a single port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance.

bridge cist {*slot/port* **|** *logical_port***} {enable | disable}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	The Link aggregate ID number (0–31).
enable	Enables Spanning Tree on the specified port for the CIST instance.
disable	Disables Spanning Tree on the specified port for the CIST instance.

Defaults

By default, the Spanning Tree status is enabled on eligible ports.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port	Implicit command for configuring the Spanning Tree status on a port for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge 1x1 slot/port	Explicit command for configuring the Spanning Tree status on a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.
vlan stp	Enables or disables the Spanning Tree instance for a VLAN.
bridge bpdu-switching	Enables or disables BPDU switching for the specified VLAN.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortEnable
```

bridge 1x1 slot/port

Enables or disables the Spanning Tree status on a single port or an aggregate of ports for the specified VLAN instance.

bridge 1x1 *vid* **{***slot/port* **|** *logical_port***} {enable | disable}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	The Link aggregate ID number (0–31).
enable	Enables Spanning Tree on the specified port for the specified instance.
disable	Disables Spanning Tree on the specified port for the specified instance.

Defaults

By default, the Spanning Tree status is enabled on eligible ports.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port	Implicit command for configuring the Spanning Tree status on a port for the flat mode CIST instance or for a 1x1 mode VLAN instance.
bridge cist slot/port	Explicit command for configuring the Spanning Tree status on a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
vlan stp	Enables or disables Spanning Tree instance for the specified VLAN.
bridge bpdu-switching	Enables or disables BPDU switching for the specified VLAN.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortEnable
```

bridge slot/port priority

Configures the Spanning Tree priority for a single port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance. The Spanning Tree Algorithm uses the port priority value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

bridge *instance* **{***slot/port* | *logical_port***} priority** *priority*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
priority	Port priority value (0–15). The lower the number, the higher the priority.

Defaults

By default, the bridge port priority value is set to 7.

Platforms Supported

OmniSwitch 6450, 6350

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 slot/port 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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port priority	Explicit command for configuring the Spanning Tree priority for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge msti slot/port priority	Explicit command for configuring the Spanning Tree priority for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port priority	Explicit command for configuring the Spanning Tree priority for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
```

bridge cist slot/port priority

Configures the Spanning Tree priority value for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. The Spanning Tree algorithm uses the port priority value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

bridge cist {*slot/port* | *logical_port***} priority** *priority*

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
priority	Port priority value (0–15). The lower the number, the higher the priority.

Defaults

By default, the bridge port priority value is set to 7.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port priority	Implicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge msti slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
```

bridge msti slot/port priority

Configures the Spanning Tree priority value for a port or an aggregate of ports for the specified flat mode Multiple Spanning Tree Instance (MSTI). The Spanning Tree algorithm uses the port priority value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

bridge msti *msti_id* **{***slot/port* | *logical_port***} priority** *priority*

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
priority	Port priority value (0–15). The lower the number, the higher the priority.

Defaults

By default, the bridge port priority value is set to 7.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port priority	Implicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge cist slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or Tree mode.
bridge 1x1 slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
```

bridge 1x1 slot/port priority

Configures the Spanning Tree priority value for a port or an aggregate of ports for the specified 1x1 mode VLAN instance. The Spanning Tree algorithm uses the port priority value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} priority** *priority*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
priority	Port priority value (0–15). The lower the number, the higher the priority.

Defaults

By default, the bridge port priority value is set to 7.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port priority	Implicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge slot/port path cost	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge msti slot/port priority	Explicit command for configuring the Spanning Tree priority value for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
```

bridge slot/port path cost

Configures the Spanning Tree path cost value for a single port or an aggregate of ports that applies to the specified flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

bridge *instance* **{***slot/port* | *logical_port***} path cost** *path_cost*

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
path_cost	Path cost value (0 - 65535 for 16-bit, 0–200000000 for 32-bit).

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6450, 6350

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 slot/port 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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge path cost mode	Selects a 32-bit or automatic path cost mode for the switch.
bridge cist slot/port path cost	Explicit command for configuring the Spanning Tree path cost for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge msti slot/port path cost	Explicit command for configuring the Spanning Tree path cost for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port path cost	Explicit command for configuring the Spanning Tree path cost for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge cist slot/port path cost

Configures the Spanning Tree path cost value for a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

bridge cist {*slot/port* | *logical_port***} path cost** *path_cost*

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
path_cost	Path cost value (0 - 65535 for 16-bit, 0–200000000 for 32-bit).

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge path cost mode	Selects a 32-bit or automatic path cost mode for the switch.
bridge slot/port path cost	Implicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge msti slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge msti slot/port path cost

Configures the Spanning Tree path cost value for a port or an aggregate of ports for the specified flat mode Multiple Spanning Tree Instance (MSTI). This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

bridge mist *msti_id* **{***slot/port* | *logical_port***} path cost** *path_cost*

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
path_cost	Path cost value (0 - 65535 for 16-bit, 0–200000000 for 32-bit).

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6450, 6350

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. Using a 16-bit path cost value is not an option.
- If zero is entered for the *path_cost* value, then 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

- If the *path_cost* value for a link aggregate is set to zero, the following default values based on link speed and link aggregate size are used:

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
10 MB	2	1,200,000
	4	800,000
	8	600,000
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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port path cost	Implicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge cist slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge 1x1 slot/port path cost

Configures the Spanning Tree path cost value for a port or an aggregate of ports for the specified 1x1 mode VLAN instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} path cost** *path_cost*

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
path_cost	Path cost value (0 - 65535 for 16-bit, 0–200000000 for 32-bit).

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 6450, 6350

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.
- 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 IEEE 892.1S recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1D Recommended Value
10 MB	2,000,000

Link Speed	IEEE 802.1D Recommended Value
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 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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port path cost	Implicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports that applies to the specified CIST or VLAN instance.
bridge cist slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge msti slot/port path cost	Explicit command for configuring the Spanning Tree path cost value for a port or an aggregate of ports for an MSTI when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPathCost
```

bridge slot/port mode

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance. Dynamic mode defers the configuration of the port state to the Spanning Tree Protocol.

bridge *instance* **{***slot/port* | *logical_port***} mode {forwarding | blocking | dynamic}**

Syntax Definitions

instance	The CIST instance or an existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
forwarding	Set port state to forwarding.
blocking	Set port state to blocking.
dynamic	Port state is determined by Spanning Tree Protocol.

Defaults

By default, the port Spanning Tree mode is set to dynamic.

Platforms Supported

OmniSwitch 6450, 6350

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 slot/port mode** command instead.
- Note that for Multiple Spanning Tree Instances (MSTI), the port Spanning Tree mode is inherited from the CIST instance and is not a configurable parameter.
- When port state is manually set to forwarding or blocking, the port remains in that state until it is changed using this command.
- Ports manually configured to operate in a forwarding or blocking state do not participate in the Spanning Tree Algorithm.

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port mode	Explicit command for configuring the Spanning Tree mode on a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat mode.
bridge 1x1 slot/port mode	Explicit command for configuring the Spanning Tree mode on a port or an aggregate of ports for a VLAN instance when the switch is operating in either the 1x1 or flat mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortManualMode
```

bridge cist slot/port mode

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or an aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

bridge cist {*slot/port* | *logical_port***} mode {dynamic | blocking | forwarding}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
dynamic	Port state is determined by Spanning Tree algorithm.
blocking	Sets port state to blocking.
forwarding	Sets port state to forwarding.

Defaults

By default, the port Spanning Tree mode is set to dynamic.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port mode	Implicit command for configuring the Spanning Tree mode for a port or an aggregate of ports for the CIST instance or a VLAN instance.
bridge 1x1 slot/port mode	Explicit command for configuring the Spanning Tree mode for a port or an aggregate of ports for the specified VLAN instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortManualMode
```

bridge 1x1 slot/port mode

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or an aggregate of ports for the specified 1x1 mode VLAN instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

bridge 1x1 *vid* **{***slot/port* | *logical_port***} mode {dynamic | blocking | forwarding}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
dynamic	Port state is determined by Spanning Tree algorithm.
blocking	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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port mode	Implicit command for configuring the Spanning Tree mode for a port or an aggregate of ports for the CIST instance or for a VLAN instance.
bridge cist slot/port mode	Explicit command for configuring the Spanning Tree mode for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortManualMode
```

bridge slot/port connection

Configures 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 | edgeport}**

Syntax Definitions

instance	The flat mode CIST instance or an existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software will automatically define connection type as point to point or no point to point.
edgeport	*This parameter is currently not supported*. Use the **bridge cist slot/port admin-edge** or **bridge cist slot/port auto-edge** command to configure edge port status.

Defaults

By default the link connection type is set to auto point to point.

Platforms Supported

OmniSwitch 6450, 6350

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 slot/port 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's connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port connection	Explicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the CIST instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.
bridge 1x1 slot/port connection	Explicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the specified VLAN instance when the switch is operating in either the 1x1 or flat Spanning Tree mode.
bridge cist slot/port admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge cist slot/port 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.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

bridge cist slot/port 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 | edgeport}**

Syntax Definitions

slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software will automatically define connection type as point to point or no point to point.
edgeport	*This parameter is currently not supported*. Use the **bridge cist slot/port admin-edge** or **bridge cist slot/port auto-edge** command to configure edge port status.

Defaults

By default, the link connection type is set to auto point to point.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the port connection type for the CIST instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in 1x1 mode when this command is used, the specified port connection type is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- A port is considered connected to a point to point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines the port should run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point to point LAN segment.
- Rapid transition of a designated port to forwarding can only occur if the port's connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

Examples

```
-> bridge mode flat
-> bridge cist 7/24 connection noptp
```

```
-> bridge mode 1x1
-> bridge cist 2/2 connection noptp
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge slot/port connection	Implicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the CIST instance or for a VLAN instance.
bridge cist slot/port admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge cist slot/port 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.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

bridge 1x1 slot/port 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 | edgeport}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	Link aggregate ID number (0–31).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software will automatically define connection type as point to point or no point to point *and* whether or not the port is an edge port.
edgeport	*This parameter is currently not supported*. Use the **bridge 1x1 slot/port admin-edge** or **bridge 1x1 slot/port auto-edge** command to configure edge port status.

Defaults

By default, the link connection type is set to auto point to point.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is an explicit Spanning Tree command that only applies to the specified VLAN instance regardless of which operating mode (flat or 1x1) is active on the switch.
- If the switch is running in the flat mode when this command is used, the specified connection type for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the 1x1 mode.
- Note that when a configuration snapshot is taken of the switch, all Spanning Tree commands are saved in their explicit format.
- A port is considered connected to a point to point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines the port should run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point to point LAN segment.
- Rapid transition of a designated port to forwarding can only occur if the port's connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

Examples

```
-> bridge mode flat
-> bridge 1x1 255 7/24 connection noptp

-> bridge mode 1x1
-> bridge 1x1 200 2/2 connection noptp
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge slot/port connection	Implicit command for configuring the Spanning Tree connection type for a port or an aggregate of ports for the CIST instance or for a VLAN instance.
bridge cist slot/port admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge cist slot/port 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.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
```

bridge cist slot/port 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 (e.g., 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 6450, 6350

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's connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

- Configure ports that will connect to a host (PC, workstation, server, etc.) as edge ports to avoid unnecessary topology changes when these ports go active. This will also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it will operationally revert back to a no point to point connection type.

Examples

```
-> bridge mode flat
-> bridge cist 15 admin-edge on
-> 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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge 1x1 slot/port admin-edge	Configures the administrative edge port status for a port or an aggregate of ports for a specific VLAN instance.
bridge cist slot/port 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 slot/port 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 slot/port 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 (e.g., 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 6450, 6350

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's 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 will connect to a host (PC, workstation, server, etc.) as edge ports to avoid unnecessary topology changes when these ports go active. This will also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it will operationally revert back to a no point to point connection type.

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge cist slot/port admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge cist slot/port 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 slot/port 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 slot/port 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 (e.g., 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 6450, 6350

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's 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 will connect to a host (PC, workstation, server, etc.) as edge ports to avoid unnecessary topology changes when these ports go active. This will also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it will operationally revert back to a no point to point connection type.

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch
bridge 1x1 slot/port 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 slot/port admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge 1x1 slot/port 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 slot/port 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 (e.g., 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 6450, 6350

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's 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 will connect to a host (PC, workstation, server, etc.) as edge ports to avoid unnecessary topology changes when these ports go active. This will also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it will operationally revert back to a no point to point connection type.

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port 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 cist slot/port admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
bridge 1x1 slot/port 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 slot/port 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 will 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 (e.g., 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 1x1 slot/port 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 slot/port 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 will 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 (e.g., 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port 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 slot/port 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 will 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 (e.g., 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge 1x1 slot/port 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 slot/port 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 will 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 (e.g., 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 6450, 6350

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 was introduced.

Related Commands

bridge mode	Selects the Spanning Tree operating mode (flat or 1x1) for the switch.
bridge cist slot/port 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 6450, 6350

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 6.6.1; command was 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

This command is used to rate limit 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 6450, 6350

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 6.6.1; command was 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 6450, 6350

Usage Guidelines

Use the **no** form of this command to disable RRSTP on the switch.

Examples

```
-> bridge rrstp
-> no bridge rrstp
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge rrstp ring	Creates a RRSTP ring comprising 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 comprising 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 6450, 6350

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 i.e. either 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 6.6.1; command was introduced.

Related Commands

bridge rrstp	Enables 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 will be over-written.

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 preconfigured 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 6450, 6350

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 has 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 6.6.1; command was introduced.

Related Commands

bridge rrstp ring	Creates a RRSTP ring comprising 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 6450, 6350

Usage Guidelines

The RRSTP status can also be modified by using **bridge rrstp ring** command.

Examples

```
-> bridge rrstp ring 1 status enable
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge rrstp ring	Creates a RRSTP ring comprising 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 (1–4094).

Defaults

parameter	default
instance	all instances

Platforms Supported

OmniSwitch 6450, 6350

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
Bridge STP Status Protocol Priority(Prio:SysID)
------+----------+--------+--------------------
    1      ON      RSTP   32768 (0x8000:0x0000
```

```
-> show spantree 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                  ON,
  Protocol             :       IEEE Rapid STP,
  mode                 : 1X1 (1 STP per Vlan),
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-2c:fa:a2:35:39:38,
  Designated Root      :   8000-2c:fa:a2:35:39:38,
  Cost to Root Bridge  :                    0,
  Root Port            :                 None,
  Next Best Root Cost  :                    0,
  Next Best Root Port  :                 None,
  TxHoldCount          :                    3,
  Topology Changes     :                    0,
  Topology age         :             00:00:00,
  Last TC Rcvd Port    :                 None,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **bridge path cost mode** command.
Bridge	The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol in the flat mode.
Spanning Tree Status	The Spanning Tree state for the CIST instance (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to 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.

output definitions (continued)

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**).
Last TC Rcvd Port	The port that received the topology change for RSTP and MSTP protocols. Default value is **None**. For linkagg, it will be displayed as *<0/linkagg_num>*.
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the **bridge max age** command.
Forward Delay	The amount of time (in seconds) that a port will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **bridge forward delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **bridge hello time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Hello Time	The Hello Time value for the root bridge.

```
-> bridge mode flat
-> bridge protocol mstp
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
 Msti STP Status Protocol Priority (Prio:SysID)
-----+----------+--------+--------------------
    0      ON      MSTP   32768 (0x8000:0x0000)
    2      ON      MSTP   32770 (0x8000:0x0002)
    3      ON      MSTP   32771 (0x8000:0x0003)
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (**32 BIT** or **AUTO**) Configured through the **bridge path cost mode** command.
Msti	The Multiple Spanning Tree Instance (MSTI) instance number. Configured through the **bridge msti** command. Note that MSTI 0 also represents the CIST instance that is always present on the switch.
Spanning Tree Status	The Spanning Tree state for the MSTI (**ON** or **OFF**).
Protocol	The Spanning Tree protocol applied to this instance. Configured through the **bridge protocol** command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the **bridge priority** command.

```
-> bridge mode 1x1
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
  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)
    4      ON        STP   32768 (0x8000)
    5      ON        STP   32768 (0x8000)
    6      ON        STP   32768 (0x8000)
    7      ON        STP   32768 (0x8000)

-> show spantree 2
Spanning Tree Parameters for Vlan 2
  Spanning Tree Status :                   ON,
  Protocol             :       IEEE STP,
  mode                 :   PVST+ (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,
  Last TC Rcvd Port    :                 None,
    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 1x1 pvst+** or **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**).
Last TC Rcvd Port	The port that received the topology change for RSTP and MSTP protocols. Default value is **None**. For linkagg, it will be displayed as *<0/linkagg_num>*.
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the **bridge max age** command.
Forward Delay	The amount of time (in seconds) that a port will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **bridge forward delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **bridge hello time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Hello Time	The Hello Time value for the root bridge.

Release History

Release 6.6.1; command was introduced.
Release 6.7.2.R02; Last TC Rcvd Port 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 mode

Displays the current global Spanning Tree mode parameter values for the switch.

show spantree mode

Syntax Definition

NA

Defaults

NA

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The global parameters for spanning tree can be activated or configured using the related commands.

Examples

```
-> show spantree mode

Spanning Tree Global Parameters
  Current Running Mode  : Per VLAN,
  Current Protocol      : N/A (Per VLAN),
  Path Cost Mode        : 32 BIT,
  Auto Vlan Containment : N/A
  Cisco PVST+ mode      : Disabled
Vlan Consistency check   : Disabled
```

output definitions

Current Running Mode	The spantree mode active on the switch. (**Flat** or **Per VLAN**)
Current Protocol	The spantree protocol active on the switch.
Path Cost Mode	The path cost mode value configured on the switch. (**AUTO** or **32 BIT**)
Auto Vlan Containment	The Auto VLAN containment mode configured on the switch (**Enabled** or **Disabled**).
Cisco PVST+ mode	The PVST+ mode configured on the switch (**Enabled** or **Disabled**).
Vlan Consistency check	Specifies if VLAN consistency check is **Enabled** or **Disabled** on the switch.

Related Commands

bridge mode	Assigns a flat Spanning Tree or per-VLAN Spanning Tree operating mode for the switch.
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 per-VLAN mode.
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 auto-vlan-containment	Enables or disables Auto VLAN Containment (AVC).

Release History

Release 6.6.4; command introduced.

MIB Objects

```
vStpTable
   vStpMode
vStpInsTable
   vStpInsProtocolSpecification
vStpBridge
   vStpPathCostMode
vStpMstRegionTable
   vStpBridgeModePVST
vStpBridge
   vStpBridgeAutoVlanContainment
```

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 6450, 6350

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 will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **bridge forward delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **bridge hello time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree	Implicit command for displaying the Spanning Tree bridge configuration for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree msti	Explicit command for displaying the Spanning Tree bridge configuration for an 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 6450, 6350

Usage Guidelines

- If an *msti_id* number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all MSTIs.
- This is an explicit Spanning Tree command that displays Spanning Tree bridge information for an MSTI regardless of which mode (1x1 or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the 1x1 mode, as MSTIs are not active in this mode. In addition, this command will fail if MSTP 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 will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. MSTIs inherit this value from the CIST instance.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. MSTIs inherit this value from the CIST instance.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree	Implicit command for displaying the Spanning Tree bridge configuration for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree cist	Explicit command for displaying the Spanning Tree bridge configuration for the CIST instance regardless of which mode (1x1 or flat) is active on the switch.
show spantree 1x1	Explicit command for displaying the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (1x1 or flat) is active on the switch.

MIB Objects

```
vStpInsTable
   vStpInsNumber
   vStpInsMode
   vStpInsProtocolSpecification
   vStpInsPriority
   vStpInsBridgeAddress
   vStpInsTimeSinceTopologyChange
   vStpInsTopChanges
   vStpInsDesignatedRoot
   vStpInsRootCost
   vStpInsRootPortNumber
   vStpInsNextBestRootCost
   vStpInsNextBestRootPortNumber
   vStpInsMaxAge
   vStpInsHelloTime
   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 6450, 6350

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 (e.g., **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 1x1
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+--------------
    1      ON        STP   32768 (0x8000)
    2      ON        STP   32768 (0x8000)
    3      ON        STP   32768 (0x8000)
    4      ON        STP   32768 (0x8000)
    5      ON        STP   32768 (0x8000)
    6      ON        STP   32768 (0x8000)
```

```
-> show spantree 1x1 7
Spanning Tree Parameters for Vlan 7
  Spanning Tree Status :                  ON,
  Protocol             :       IEEE STP,
  mode                 : 1X1 (1 STP per Vlan),
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-00:d0:95:6a:f4:58,
  Designated Root      :   0000-00:00:00:00:00:00,
  Cost to Root Bridge  :                    0,
  Root Port            :   Slot 1 Interface 1,
  Next Best Root Cost  :                    0,
  Next Best Root Port  :   Slot 1 Interface 1,
  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

-> 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 will remain in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the **bridge forward delay** command.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the **bridge hello time** command.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree	Implicit command for displaying the Spanning Tree bridge configuration for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree cist	Explicit command for displaying the Spanning Tree bridge configuration for the CIST instance regardless of which mode (1x1 or flat) is active on the switch.
show spantree msti	Explicit command for displaying the Spanning Tree bridge information for an 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 6450, 6350

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

```
-> bridge mode flat
-> show spantree ports
Bridge Port  Oper Status  Path Cost  Role
------+-----+------------+---------+-----
    1  1/1      FORW          19   ROOT
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12      DIS           0    DIS

-> show spantree 1 ports
Spanning Tree Port Summary
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+-----+---+---+---------------------
 1/1  FORW      19      52 ROOT  1/1  PTP EDG 8000-00:30:f1:5b:37:73
 1/2   DIS       0       0  DIS  1/2   NS  NO 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS  1/3   NS  NO 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS  1/4   NS  NO 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS  1/5   NS  NO 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS  1/6   NS  NO 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS  1/7   NS  NO 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS  1/8   NS  NO 0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS  1/9   NS  NO 0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS  1/10  NS  NO 0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS  1/11  NS  NO 0000-00:00:00:00:00:00
 1/12  DIS       0       0  DIS  1/12  NS  NO 0000-00:00:00:00:00:00

-> show spantree 1 ports active
Spanning Tree Port Summary
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+-----+---+---+---------------------
 1/1  FORW      19      52 ROOT 1/1   PTP EDG 8000-00:30:f1:5b:37:73
```

output definitions

Bridge	The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol in the flat mode.
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, learning, and forwarding.

output definitions (continued)

Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge slot/port path cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.
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** (non significant)**.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
 -> show spantree msti 1 ports configured
Spanning Tree Port Admin Configuration
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr
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 (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.

output definitions

Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge slot/port path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT**. Configured through the **bridge slot/port 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 slot/port 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 slot/port auto-edge** or **bridge 1x1 slot/port 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 slot/port restricted-tcn** or **bridge 1x1 slot/port 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 slot/port restricted-role** or **bridge 1x1 slot/port restricted-role** command.
10G Opt.	N/A

```
-> bridge mode flat
-> bridge protocol mstp
-> show spantree ports
 Msti  Port Oper Status  Path Cost  Role
-----+-----+------------+---------+-----
    0  1/1      FORW       200000   ROOT
    0  1/2       DIS           0    DIS
    0  1/3       DIS           0    DIS
    0  1/4       DIS           0    DIS
    0  1/5       DIS           0    DIS
    0  1/6       DIS           0    DIS
    0  1/7       DIS           0    DIS
    0  1/8       DIS           0    DIS
    0  1/9       DIS           0    DIS
    0  1/10      DIS           0    DIS
    0  1/11      DIS           0    DIS
    0  1/12      DIS           0    DIS
    0  1/13      DIS           0    DIS
    0  1/14      DIS           0    DIS
    0  1/15      DIS           0    DIS
    0  1/16      DIS           0    DIS
    0  1/17      DIS           0    DIS
    0  1/18      DIS           0    DIS
    0  1/19      DIS           0    DIS
    0  1/20      DIS           0    DIS
    0  1/21      DIS           0    DIS
```

```
    0  1/22      DIS           0    DIS
    0  1/23      DIS           0    DIS
    0  1/24      DIS           0    DIS
    0  5/1       DIS           0    DIS
    0  5/2       DIS           0    DIS
    1  1/1       FORW     200000    MSTR
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12      DIS           0    DIS
    1  1/13      DIS           0    DIS
    1  1/14      DIS           0    DIS
    1  1/15      DIS           0    DIS
    1  1/16      DIS           0    DIS
    1  1/17      DIS           0    DIS
    1  1/18      DIS           0    DIS
    1  1/19      DIS           0    DIS
    1  1/20      DIS           0    DIS
    1  1/21      DIS           0    DIS
    1  1/22      DIS           0    DIS
    1  1/23      DIS           0    DIS
    1  1/24      DIS           0    DIS

-> show spantree ports active
 Msti  Port Oper Status  Path Cost  Role
-----+-----+------------+---------+-----
    0  1/1      FORW       200000   ROOT
    1  1/1      FORW       200000   MSTR
    2  1/1      FORW       200000   MSTR
```

output definitions

Msti	The Multiple Spanning Tree Instance (MSTI) instance number. Configured through the **bridge msti** command. Note that MSTI 0 also represents the CIST instance that is always present on the switch.
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge slot/port path cost** command.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.

```
-> bridge mode 1x1
-> show spantree ports
 Vlan  Port Oper Status  Path Cost  Role
-----+-----+-----------+---------+-----
    1  1/1       DIS           0    DIS
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12     FORW          19    ROOT
-> show spantree 1 ports
Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+----+---+----+---------------------
 1/1   DIS       0       0  DIS 1/1   NS EDG  0000-00:00:00:00:00:00
 1/2   DIS       0       0  DIS 1/2   NS  NO  0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS 1/3   NS  NO  0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS 1/4   NS  NO  0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS 1/5   NS  NO  0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS 1/6   NS  NO  0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS 1/7   NS  NO  0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS 1/8   NS  NO  0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS 1/9   NS  NO  0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS 1/10  NS  NO  0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS 1/11  NS  NO  0000-00:00:00:00:00:00
 1/12 FORW      19       0 ROOT 1/12 PTP  NO  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
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+----+---+---+---------------------
 1/12 FORW      19       0 ROOT 1/12 PTP  EDG 0001-00:d0:95:6a:79:50
```

output definitions

Vlan	The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the **vlan** commands
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge slot/port path cost** command.

output definitions (continued)

Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **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** (non significant)**.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree 2 ports configured
Spanning Tree Port Admin Configuration for Vlan 2
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr      PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Role 10G Opt.  Cfg Stst
-----+----+----+----+-------+----+----+----+----+----+---------+---------
 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 (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.
Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge slot/port path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT.** Configured through the **bridge slot/port 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 slot/port 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 slot/port auto-edge** or **bridge 1x1 slot/port 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 slot/port restricted-tcn** or **bridge 1x1 slot/port 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 slot/port restricted-role** or **bridge 1x1 slot/port restricted-role** command.
10G Opt.	N/A
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 6.6.1; command was introduced.

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 6450, 6350

Usage Guidelines

- This is an explicit Spanning Tree command that displays Spanning Tree port information for the flat mode CIST instance regardless of which mode (1x1 or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the 1x1 mode, as the CIST is not active in this mode.

Examples

```
-> show spantree cist ports
Spanning Tree Port Summary for Cist
      Oper  Path   Desig        Prim. Op Op
Port   St   Cost    Cost   Role Port Cnx Edg   Desig Bridge ID
-----+----+-------+-------+----+----+---+----+---------------------
 1/1  FORW  200000      52 ROOT 1/1  PTP  EDG  8000-00:30:f1:5b:37:73
 1/2   DIS       0       0  DIS 1/2   NS   No  0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS 1/3   NS  EDG  0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS 1/4   NS   No  0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS 1/5   NS  EDG  0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS 1/6   NS  EDG  0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS 1/7   NS  EDG  0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS 1/8   NS   No  0000-00:00:00:00:00:00
```

```
-> show spantree cist ports active
Spanning Tree Port Summary for Cist
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg  Desig Bridge ID
-----+----+-------+-------+----+----+----+----+--------------------
1/1  FORW  200000      52 ROOT  1/1  PTP  EDG  8000-00:30:f1:5b:37:73
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge slot/port path cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate**, and **backup**.
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** (non significant). Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree cist ports configured
Spanning Tree Port Admin Configuration for Vlan 1
      Port  Adm  Man. Config  Adm  Adm  Aut  Rstr  Rstr Role/          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 (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.
Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge slot/port path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT.** Configured through the **bridge slot/port 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 slot/port 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 slot/port auto-edge** or **bridge 1x1 slot/port 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 slot/port restricted-tcn** or **bridge 1x1 slot/port 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 slot/port restricted-role** or **bridge 1x1 slot/port restricted-role** command.
10G Opt.	N/A
PVST+ Cfg Stat	The PVST+ status on the switch: **enabled** or **disabled**. Configured through the **bridge mode 1x1 pvst+** 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 **bridge mode 1x1 pvst+** command.

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree ports	Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree msti ports	Explicit command for displaying Spanning Tree port information for an 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 6450, 6350

Usage Guidelines

- If an *msti_id* number is *not* specified, this command displays the Spanning Tree port operational status, path cost, and role values for all associated MSTIs.
- This is an explicit Spanning Tree command that displays Spanning Tree port information for an MSTI regardless of which mode (1x1 or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the 1x1 mode, as MSTIs are not active in this mode. In addition, if MSTP is not the selected flat mode protocol, this command will fail.
- The **configured** keyword is only available when an instance number is specified with this command. In addition, this keyword cannot be used in combination with either the **forwarding** or **blocking** keywords.
- Note that MSTI 0 also represents the CIST instance that is always present on the switch. To view the CIST instance using this command, specify zero (0) for the *msti_id* number.

Examples

```
-> show spantree msti ports
 Msti  Port Oper Status  Path Cost  Role
-----+-----+-----------+---------+-----
    0  1/1      FORW       200000   ROOT
    0  1/2       DIS           0    DIS
    0  1/3       DIS           0    DIS
    0  1/4       DIS           0    DIS
    0  1/5       DIS           0    DIS
    0  1/6       DIS           0    DIS
    0  1/7       DIS           0    DIS
    0  1/8       DIS           0    DIS
    0  1/9       DIS           0    DIS
    0  1/10      DIS           0    DIS
    0  1/11      DIS           0    DIS
    0  1/12      DIS           0    DIS
    0  1/13      DIS           0    DIS
    0  1/14      DIS           0    DIS
    0  1/15      DIS           0    DIS
    0  1/16      DIS           0    DIS
    0  1/17      DIS           0    DIS
    0  1/18      DIS           0    DIS
    0  1/19      DIS           0    DIS
    0  1/20      DIS           0    DIS
    0  1/21      DIS           0    DIS
    0  1/22      DIS           0    DIS
    0  1/23      DIS           0    DIS
    0  1/24      DIS           0    DIS
    0  5/1       DIS           0    DIS
    0  5/2       DIS           0    DIS
    1  1/1      FORW       200000   MSTR
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12      DIS           0    DIS
    1  1/13      DIS           0    DIS
    1  1/14      DIS           0    DIS
    1  1/15      DIS           0    DIS
    1  1/16      DIS           0    DIS
    1  1/17      DIS           0    DIS
    1  1/18      DIS           0    DIS
    1  1/19      DIS           0    DIS
    1  1/20      DIS           0    DIS
    1  1/21      DIS           0    DIS
    1  1/22      DIS           0    DIS
    1  1/23      DIS           0    DIS
    1  1/24      DIS           0    DIS
    1  5/1       DIS           0    DIS
    1  5/2       DIS           0    DIS
```

```
-> show spantree msti 2 ports
Spanning Tree Port Summary for Msti 2
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+-----+---+---+----------------------
 1/1  FORW  200000       0 MSTR 1/1   PTP EDG 8002-00:d0:95:57:3a:9e
 1/2   DIS       0       0  DIS 1/2   NS  NO 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS 1/3   NS  NO 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS 1/4   NS  NO 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS 1/5   NS  NO 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS 1/6   NS  NO 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS 1/7   NS  NO 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS 1/8   NS  NO 0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS 1/9   NS  NO 0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS 1/10  NS  NO 0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS 1/11  NS  NO 0000-00:00:00:00:00:00
 1/12  DIS       0       0  DIS 1/12  NS  NO 0000-00:00:00:00:00:00
 1/13  DIS       0       0  DIS 1/13  NS  NO 0000-00:00:00:00:00:00
 1/14  DIS       0       0  DIS 1/14  NS  NO 0000-00:00:00:00:00:00
 1/15  DIS       0       0  DIS 1/15  NS  NO 0000-00:00:00:00:00:00
 1/16  DIS       0       0  DIS 1/16  NS  NO 0000-00:00:00:00:00:00
 1/17  DIS       0       0  DIS 1/17  NS  NO 0000-00:00:00:00:00:00
 1/18  DIS       0       0  DIS 1/18  NS  NO 0000-00:00:00:00:00:00
 1/19  DIS       0       0  DIS 1/19  NS  NO 0000-00:00:00:00:00:00
 1/20  DIS       0       0  DIS 1/20  NS  NO 0000-00:00:00:00:00:00
 1/21  DIS       0       0  DIS 1/21  NS  NO 0000-00:00:00:00:00:00
 1/22  DIS       0       0  DIS 1/22  NS  NO 0000-00:00:00:00:00:00
 1/23  DIS       0       0  DIS 1/23  NS  NO 0000-00:00:00:00:00:00
 1/24  DIS       0       0  DIS 1/24  NS  NO 0000-00:00:00:00:00:00
 5/1   DIS       0       0  DIS 5/1   NS  NO 0000-00:00:00:00:00:00
 5/2   DIS       0       0  DIS 5/2   NS  NO 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
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+-----+---+---+----------------------
 1/1  FORW  200000       0 MSTR 1/1   PTP EDG 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 (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge msti slot/port path cost** command.

output definitions (continued)

Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
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** (non significant). Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree msti 2 ports configured
Spanning Tree Port Admin Configuration for Msti 2
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr
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 (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge msti slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.

output definitions (continued)

Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge msti slot/port path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT.** Configured through the **bridge slot/port 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 slot/port 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 slot/port auto-edge** or **bridge 1x1 slot/port 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 slot/port restricted-tcn** or **bridge 1x1 slot/port 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 slot/port restricted-role** or **bridge 1x1 slot/port restricted-role** command.
10G Opt.	N/A

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree ports	Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree cist ports	Explicit command for displaying Spanning Tree port information for a CIST instance when the switch is operating in the 1x1 or flat Spanning Tree mode.
show spantree 1x1 ports	Explicit command for displaying Spanning Tree port information for a VLAN when the switch is operating in the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortState
   vStpInsPortEnable
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortDesignatedBridge
   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 6450, 6350

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 (e.g., **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
-----+-----+------------+---------+-----
    1  1/1       DIS           0    DIS
    1  1/2       DIS           0    DIS
    1  1/3       DIS           0    DIS
    1  1/4       DIS           0    DIS
    1  1/5       DIS           0    DIS
    1  1/6       DIS           0    DIS
    1  1/7       DIS           0    DIS
    1  1/8       DIS           0    DIS
    1  1/9       DIS           0    DIS
    1  1/10      DIS           0    DIS
    1  1/11      DIS           0    DIS
    1  1/12     FORW          19    DIS


-> show spantree 1x1 1 ports
Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+-----+---+---+----------------------
 1/1   DIS       0       0  DIS  1/1   NS EDG 0000-00:00:00:00:00:00
 1/2   DIS       0       0  DIS  1/2   NS  NO 0000-00:00:00:00:00:00
 1/3   DIS       0       0  DIS  1/3   NS  NO 0000-00:00:00:00:00:00
 1/4   DIS       0       0  DIS  1/4   NS  NO 0000-00:00:00:00:00:00
 1/5   DIS       0       0  DIS  1/5   NS  NO 0000-00:00:00:00:00:00
 1/6   DIS       0       0  DIS  1/6   NS  NO 0000-00:00:00:00:00:00
 1/7   DIS       0       0  DIS  1/7   NS  NO 0000-00:00:00:00:00:00
 1/8   DIS       0       0  DIS  1/8   NS  NO 0000-00:00:00:00:00:00
 1/9   DIS       0       0  DIS  1/9   NS  NO 0000-00:00:00:00:00:00
 1/10  DIS       0       0  DIS  1/10  NS  NO 0000-00:00:00:00:00:00
 1/11  DIS       0       0  DIS  1/11  NS  NO 0000-00:00:00:00:00:00
 1/12 FORW      19       0  DIS  1/12 PTP  NO 0001-00:d0:95:6a:79:50


-> show spantree 1x1 1 ports active
Spanning Tree Port Summary for Vlan 1
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+----+---+---+----------------------
 1/12 FORW      19       0  DIS 1/12 PTP EDG 0001-00:d0:95:6a:79:50


-> show spantree 1x1 10-13 ports
Spanning Tree Port Summary for Vlan 10
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Egd Desig Bridge ID
-----+----+-------+-------+----+----+----+---+----------------------
 1/46  DIS       0       0  DIS 1/46  NS  EDG 0000-00:00:00:00:00:00
Spanning Tree Port Summary for Vl 11
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+-----+---+---+--------------------
 1/36  DIS       0       0  DIS 1/36  NS EDG 0000-00:00:00:00:00:00
 1/37  DIS       0       0  DIS 1/37  NS  NO 0000-00:00:00:00:00:00
```

```
Spanning Tree Port Summary for Vlan 12
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+-----+---+---+---------------------
 1/42  DIS       0       0  DIS 1/42  NS  EDG 0000-00:00:00:00:00:00
 1/43  DIS       0       0  DIS 1/43  NS   NO 0000-00:00:00:00:00:00
Spanning Tree Port Summary for Vlan 13
      Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID
-----+----+-------+-------+----+-----+---+---+---------------------
 1/38  DIS       0       0  DIS 1/38  NS  EDG 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 (e.g., 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the **bridge 1x1 slot/port path cost** command.
Desig Cost	The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
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** (non significant). Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Op Edg	Operational connection type: **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.

```
-> show spantree 1x1 1 ports configured
Spanning Tree Port Admin Configuration for Vlan 1
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/           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
 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

-> show spantree 1x1 10-13 ports configured
Spanning Tree Port Admin Configuration for Vlan 10
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/           PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  10G Opt  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+--------+---------
 1/46    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/           PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  10G Opt  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+---------+--------+---------
 1/36    7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF
 1/37    7  ENA  No        0  AUT   No  Yes   No    No        DIS     AUT OFF
Spanning Tree Port Admin Configuration for Vlan 12
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/           PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  10G Opt  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+----------+--------+---------
 1/42    7  ENA  No        0  AUT   No  Yes  No     No         DIS     AUT OFF
 1/43    7  ENA  No        0  AUT   No  Yes  No     No         DIS     AUT OFF
Spanning Tree Port Admin Configuration for Vlan 13
      Port  Adm Man. Config  Adm  Adm  Aut  Rstr Rstr Role/           PVST+
Port  Pri   St. Mode   Cost  Cnx  Edg  Edg  Tcn  Root Guard  10G Opt  Cfg Stat
-----+----+----+----+-------+----+----+-----+----+----------+--------+---------
 1/38    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 (e.g., 0/31).
Port Pri	The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the **bridge 1x1 slot/port priority** command.
Adm St	The Spanning Tree administrative status of the port: **enabled** or **disabled**. Configured through the **bridge slot/port** command to enable or disable Spanning Tree on a port.

output definitions (continued)

Man. Mode	The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the **bridge slot/port mode** command.
Config Cost	The configured path cost value for this port. Configured through the **bridge 1x1 slot/port path cost** command.
Adm Cnx	The administrative connection type: **PTP, NPT,** or **AUT**. Configured through the **bridge slot/port 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 slot/port 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 slot/port auto-edge** or **bridge 1x1 slot/port 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 slot/port restricted-tcn** or **bridge 1x1 slot/port 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 slot/port restricted-role** or **bridge 1x1 slot/port restricted-role** command.
10G Opt.	N/A
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 through the **bridge mode 1x1 pvst+** command.

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree ports	Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a 1x1 mode VLAN instance.
show spantree cist ports	Explicit command for displaying Spanning Tree port information for a CIST instance when the switch is operating in the 1x1 or flat Spanning Tree mode.
show spantree msti ports	Explicit command for displaying Spanning Tree port information for an MSTI when the switch is operating in the 1x1 or flat Spanning Tree mode.

MIB Objects

```
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortPriority
   vStpInsPortState
   vStpInsPortEnable
   vStpInsPortPathCost
   vStpInsPortDesignatedCost
   vStpInsPortDesignatedBridge
   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 6450, 6350

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   : Region 1
Revision Level       : 0
Configuration Digest : 0xac36177f 50283cd4 b83821d8 ab26de62
Revision Max hops    : 20
Cist Instance Number : 0
```

output definitions

Configuration Name	An alphanumeric string up to 32 characters that identifies the name of the MST region. Use the **bridge mst region name** command to define this value.
Revision Level	A numeric value (0–65535) that identifies the MST region revision level for the switch.
Configuration Digest	An MST region identifier consisting of a 16 octet hex value (as per the IEEE 802.1Q 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 that this instance is also known as the flat mode instance and is known as bridge 1 when using STP or RSTP.

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstRegionTable
   vStpMstRegionNumber
   vStpMstRegionConfigDigest
   vStpMstRegionConfigName
   vStpMstRegionConfigRevisionLevel
   vStpMstRegionCistInstanceNumber
   vStpMstRegionMaxHops
```

show spantree msti vlan-map

Displays the range of VLANs associated with the specified Multiple Spanning Tree Instance (MSTI).

show spantree mst [*msti_id***] vlan-map**

Syntax Definitions

msti_id	An existing MSTI ID number (0–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If an *msti_id* is not specified, then the VLAN to MSTI mapping for all defined MSTIs is displayed.
- This command is available when the switch is operating in either the 1x1 or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance (also known as MSTI 0).

Examples

```
-> show spantree msti vlan-map
 Spanning Tree Msti/Cist Vlan map
----------------------------------

 Cist
 Name                :
 VLAN list           : 1-9,14-4094

 Msti 1
 Name                :
 VLAN list           : 10-11

 Msti 2
 Name                :
 VLAN list           : 12-13

-> show spantree msti 2 vlan-map
 Spanning Tree Msti Vlan map
-----------------------------

 Msti 2
 Name                :
 VLAN list           : 12-13
```

output definitions

Cist Instance	Identifies MSTI VLAN mapping information for the CIST instance.
Msti	The MSTI ID number that identifies an association between a Spanning Tree instance and a range of VLANs.
Name	An alphanumeric value that identifies an MSTI name. Use the **bridge msti** command to define an MSTI name.
VLAN list	The range of VLAN IDs that are associated with this MSTI.

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree mst region	Displays the MST region information for the switch.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapState
```

show spantree cist vlan-map

Displays the range of VLANs associated with the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist vlan-map

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is available when the switch is operating in either the 1x1 or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance 0 (also known as MSTI 0).

Examples

```
-> show spantree cist vlan-map
 Spanning Tree Cist Vlan map
----------------------------

 Cist
 Name           :
 VLAN list      : 1-9,14-4094
```

output definitions

Name	An alphanumeric value that identifies the name of the CIST. Use the **bridge msti** command to define a name for this instance.
VLAN list	The range of VLAN IDs that are associated with the CIST instance.

Release History

Release 6.6.1; command was introduced.

Related Commands

show spantree mst region	Displays the MST region information for the switch.
show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstInstanceTable
   vStpMstInstanceNumber
   vStpMstInstanceName
   vStpMstInstanceVlanBitmapState
```

show spantree map-msti

Displays the Multiple Spanning Tree Instance (MSTI) that is associated to the specified VLAN.

show spantree mst *vid* **vlan-map**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

show spantree mst region	Displays the MST region information for the switch.
show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.

MIB Objects

```
vStpMstVlanAssignmentTable
   vStpMstVlanAssignmentVlanNumber
   vStpMstVlanAssignmentMstiNumber
```

show spantree mst port

Displays a summary of Spanning Tree connection information and instance associations for the specified port or a link aggregate of ports.

show spantree mst port {*slot/port* **|** *logical_port***}**

Syntax Definitions

slot/port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
logical_port	The Link aggregate ID number (0–31).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is only available when the switch is running in the flat Spanning Tree mode.
- Note that MST 0 also represents the flat mode CIST instance, which all ports are associated with when the switch is running in the flat Spanning Tree mode.

Examples

```
-> bridge mode flat
-> show spantree mst port 1/10
MST parameters for interface 1/10:
  Conection Type:  NS
  Edge Port: YES
  Boundary Port: YES

 MST |  Role  | State | Pth Cst | Vlans
-----------------------------------------------------
 0       DIS      DIS          0   200
 2       DIS      DIS          0

-> show spantree mst port 1/1
MST parameters for interface 1/1 :
  Conection Type: PTP
  Edge Port: NO
  Boundary Port: YES

 MST |  Role  | State | Pth Cst | Vlans
-----------------------------------------------------
 0      ROOT     FORW         19   1
-> bridge mode 1x1
-> show spantree mst port 1/10
Current STP mode is 1x1, MSTI instances are inactive
```

output definitions

Connection Type	Operational connection type: **PTP, NPT**, **NS** (non-significant) or **EDG.** Shows the current operational state of the port's connection type. See the **bridge slot/port connection** command on page 16-87 for more information.
Edge Port	Indicates whether or not the port is an edge port (**YES** or **NO**).
Boundary Port	Indicates whether or not the port is a boundary port (**YES** or **NO**). A boundary port connects an MST bridge to a LAN that belongs to a different MST region.
MST	The Multiple Spanning Tree Instance (MSTI) number that is associated with this port.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: **root, designated, alternate, master**, and **backup**.
State	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Pth Cst	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.
Vlans	The VLAN ID of the default VLAN for the port.

Release History

Release 6.6.1; command was 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

```
vStpInsPortTable
   vStpInsPortAdminConnectionType
   vStpInsPortAdminEdge
   vStpInsPortAutoEdge
   vStpMstInstanceNumber
   vStpInsPortRole
   vStpInsPortState
   vStpInsPortPathCost
vStpMstVlanAssignmentTable
   vStpMstVlanAssignmentVlanNumber
```

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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show bridge rrstp configuration
RRSTP Global state is Enabled
```

Release History

Release 6.6.1; command was introduced.

Related Commands

bridge rrstp	Enables 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 present in the system.

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

bridge rrstp ring	Creates a RRSTP ring comprising of two ports.
show bridge rrstp configuration	Displays the current RRSTP status for the switch.

MIB Objects

```
vStpRrstpRingConfigTable
   vStpRrstpRingId
   vStpRrstpRingPort1
   vStpRrstpRingPort2
   vStpRrstpRingVlanTag
   vStpRrstpRingState
   vStpRrstpRingRowStatus
```

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 6450, 6350

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 6.6.1; command was 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 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 (e.g., 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 will be used.
disable	Specifies that IEEE BPDUs will be used.

Defaults

parameters	default
auto | enable | disable	**auto**

Platforms Supported

OmniSwitch 6450, 6350

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 will send and receive 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 was introduced.

Related Commands

bridge mode 1x1 pvst+	Enables or disables PVST+ mode on the switch.

MIB Objects

```
vStpPortConfigTable
   vStpPortConfigIfInedx
   vStpPortConfigPVST
```

17 Ethernet Ring Protection Commands

Ethernet Ring Protection (ERP) is a protection switching mechanism for Ethernet ring topologies, such as multi-ring and ladder networks. This implementation of ERP is based on Recommendation ITU-T G.8032/ Y.1344 and uses the ring Automatic Protection Switching (APS) protocol to coordinate the prevention of 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 the Ethernet ring protection command is as follows:

Filename: AlcatelIND1Erp.mib
Module: ALCATEL-IND1-ERP-MIB

A summary of available commands is listed here:

erp-ring
erp-ring sub-ring-port
erp-ring protected-vlan (deprecated)
erp-ring rpl-node
erp-ring wait-to-restore
erp-ring enable
erp-ring ethoam-event remote-endpoint
erp-ring guard-timer
erp-ring virtual-channel
erp-ring revertive
erp-ring reset-version-fallback
erp-ring clear
clear erp statistics
show erp
show erp protected-vlan (deprecated)
show erp statistics

erp-ring

Creates an Ethernet Ring Protection (ERP) ring 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 and 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- 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- 4094.
level_num	The MEG level number for the service VLAN. The valid range is 0-7.
guard-timer	The guard timer value, in centi-secs, 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 6450

Usage Guidelines

- Use the **no** form of this command to remove a ring from the switch configuration. Note that administratively disabling ring ports is recommended before deleting the ring to avoid creating any network loops. Once the ring is deleted, then ensure that the same ports are administratively enabled under Spanning Tree control.
- The specified ring identification number must be unique within a switch.
- 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.)
- VPA (default or 802.1Q tagged) must be configured for the ring port.

- 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.
- A port can be configured in the ERP ring only when the port is tagged to the service VLAN.
- 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.
- ERPv2 and STP shall not operate together on the same port. All the VLANs tagged to the ring port (802.1q) shall be controlled by ERP only and not by STP.

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 6.6.2; command was introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.
show erp protected-vlan	Displays the protected VLAN configuration for the switch.
show erp statistics	Displays ERP ring statistics.
ethernet-service svlan nni	Creates a NNI-SVLAN binding.

MIB Objects

```
alaErpRingId
   alaErpRingServiceVid
   alaErpRingMEGLevel
   alaErpRingStatus
   alaErpRingPort1
   alaErpRingPort2
   alaErpRingGuardTimer
   alaErpRingRowStatus
```

erp-ring sub-ring-port

This command configures a sub-ring on the interconnection node. Sub-ring port along with the service VLAN and MEG level will have to be specified. There will be only one port as a part of sub-ring on the interconnection node. Other ring ports will be a part of major ring and not the 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 6450

Usage Guidelines

- Use the **no** form of this command to remove a sub-ring from the switch configuration. Administratively 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.
- 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.
- 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 service-vlan 10 level 2 enable

-> no erp-ring 2
```

Release History

Release 6.7.2.R03; 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
   alaErpRingGuardTimer
   alaErpRingRowStatus
```

erp-ring protected-vlan

Configures a VLAN as a protected VLAN for an ERP ring. The ring ports associated with the specified ring ID are tagged with the protected VLAN ID.

erp-ring *ring_id* **protected-vlan** *vlan_id1***[**-*vlan_id2***] [***vlan_id1***[**-*vlan_id2***]]**

no erp-ring *ring_id* **protected-vlan [***vlan_id1***[**-*vlan_id2***]]**

Syntax Definitions

ring_id	The ERP ring ID number. The valid range is 1- 2147483647.
vlan_id1[-vlan_id2]	The VLAN ID number. To specify multiple VLAN IDs in a single command, use a hyphen to indicate a contiguous range of VLAN IDs and a space to separate multiple VLAN ID entries (for example, 10-20 30 100).

Defaults

NA

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use the **no** form of this command to remove a protected VLAN from the ERP ring configuration.
- The ERP ring ID number specified must already exist in the switch configuration, unless the VLAN ID specified belongs to a VLAN Stacking SVLAN.
- The VLAN ID specified must already exist in the switch configuration.
- Specify only static VLAN IDs; dynamic VLANs are not configurable as protected VLANs.
- A protected VLAN can belong to only one ERP ring at a time.
- The specified protected VLAN ID must not participate in a Spanning Tree instance that is associated with non-ERP VLANs. This may require changing the Spanning Tree configuration for the VLAN ID prior to using this command.
- A SVLAN with two ERP VPA type NNI ports is automatically configured as an ERP protected VLAN on a ring if the two NNI ports constitute its ring ports.
- Deletion of SVLAN-NNI binding results in removal of the SVLAN from the corresponding ERP protected VLAN database.

Examples

```
-> erp-ring 1 protected-vlan 11
-> erp-ring 1 protected-vlan 12-20 25-40 100
-> erp-ring 2 protected-vlan 30-50
-> no erp-ring 1 protected-vlan
```

```
-> no erp-ring 1 protected-vlan 25-40
```

Release History

Release 6.6.2; command was introduced.
Release 6.7.2.R03; command deprecated.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.
show erp protected-vlan	Displays the protected VLAN configuration for the switch.

MIB Objects

```
alaErpRingId
alaErpRingVlanProtectedVid
alaErpRingVlanRowStatus
```

erp-ring rpl-node

Configures a switch as a Ring Protection Link (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 valid range is 1- 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

N/A

Platforms Supported

OmniSwitch 6450

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 configuration applied to the ring while it is enabled is rejected.
- The specified ERP ring ID must already 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.

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 6.6.2; command was 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

```
alaErpRingId
alaErpRingPortIfIndex
alaErpRingPortType
```

erp-ring wait-to-restore

Configures the wait-to-restore timer value for the Ring Protection Link (RPL) switch. This timer determines the number of 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- 2147483647.
wtr_timer	The number of minutes to wait before restoring the RPL to a blocked state. The valid range is 1-12.

Defaults

By default, the wait-to-restore timer value is set to 5 minutes.

Platforms Supported

OmniSwitch 6450

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 already 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 6.6.2; command was 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 1- 2147483647.

Defaults

By default, ERP rings are disabled when they are created.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The specified ring ID must already 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 6.6.2; command was 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 ethoam-event remote-endpoint

Configures an ERP ring port to accept or drop a loss of connectivity event for a Remote Ethernet OAM Maintenance End Point (MEP). This command allows ERP to interact with Ethernet OAM to monitor non-ERP nodes that may exist in an ERP ring.

erp-ring *ring_id* **ethoam-event {port** *slot/port* **| linkagg** *agg_num***} remote-endpoint** *mep_id*

no erp-ring *ring_id* **ethoam-event {port** *slot/port* **| linkagg** *agg_num***}**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1- 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 MEP ID number. The valid range is 1-8191.

Defaults

By default, ERP ports drops Ethernet OAM loss of connectivity events.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use the **no** form of this command to configure the ERP ring port to drop loss of connectivity events.
- The specified ring ID must already exist in the switch configuration.
- The specified remote MEP ID number is only allowed on one ring port within the same ERP ring.
- Maintenance Domain of level same as ring MEG Level, Maintenance Association of VLAN ID same as service VLAN ID, down MEP on port on which ETH OAM event must be configured. RMEP-ID in MEP-LIST database must be configured for successful ETH OAM event registration.

Examples

```
-> erp-ring 1 ethoam-event port 1/1 remote-endpoint 10
-> erp-ring 1 ethoam-event linkagg 1 remote-endpoint 20
-> no erp-ring 1 ethoam-event port 1/1
```

Release History

Release 6.6.2; command was introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId
alaErpRingPortEthOAMEvent
alaErpRingPortRmepId
```

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 6450

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 already exist in the switch configuration.

Examples

```
-> erp-ring 1 guard-timer 10
-> no erp-ring 1 guard-timer
```

Release History

Release 6.6.2; command was 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 virtual-channel

Enables or disables an ERP 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 6450

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.
- Virtual Channel must be configured only in the sub-ring. For major ring, virtual channel must always be enabled, which is the default value.
- The Virtual Channel configuration (enable / disable) must be consistent for all the sub-rings nodes including the RPL owner.

Examples

```
-> erp-ring 2 virtual-channel disable
-> erp-ring 1 virtual-channel enable
```

Release History

Release 6.7.2.R03; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring-port	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**.** When enabled, 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. When disabled, 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 6450

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 6.7.2.R03; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring rpl-node	Configures a switch as a Ring Protection Link (RPL) node.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingRevertive
```

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 6450

Usage Guidelines

- Use this command after upgrading OmniSwitch to the latest AOS version. This command must be issued on all nodes in a ring, starting from the RPL node as part of the ERPv2 upgradation process. Refer to the Release Notes for more information on the upgrade procedure.
- 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 6.7.2.R03; command introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingActiveVersion
   alaErpRingResetVersionFallback
```

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 6450

Usage Guidelines

The specified ring identification number must be unique within a switch.

Examples

```
-> erp-ring 1 clear
```

Release History

Release 6.7.2.R03; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring rpl-node	Configures a switch as a Ring Protection Link (RPL) node.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingTable
   alaErpRingId
   alaErpRingClearAction
```

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- 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 6450

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 already 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 6.6.2; command was 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- 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 6450

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 already exist in the switch configuration.

Examples

```
-> show erp
Legends: *   - Inactive Configuration
         WTR - Wait To Restore
         MEG - 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

cli> show erp ring 302
Ring Id                 : 1,
Ring Type               : Normal Ring,
Ring Port1              : 2/4,
Ring Port2              : 2/6,
Ring Status             : enabled,
```

```
Service VLAN           : 10,
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,
Time to Revert         : 0,
Ring Node Type         : non-rpl,
Last State Change      : WED AUG 10 07:03:30 2011  (sysUpTime 22d:03h:45m)
```

output definitions

Ring ID	The ERP ring ID number.
Ring Type	The ring type.
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.
Revertive Mode	The revertive mode status **(enabled** or **disabled)**.
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.
Virtual Channel	The virtual channel status **(enabled** or **disabled)**.
MEG Level	The Service VLAN Management Entity Group (MEG) level.
Ring State	Indicates the state of the ring.
Active ERP version	The active ERP version.
Time to Revert	Indicates the time left for WTR to get expired.
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 1/15
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 accepts 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 6.6.2; command was introduced.

Related Commands

show erp protected-vlan	Displays the protected VLAN configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingId
alaErpRingStatus
alaErpRingServiceVid
alaErpRingMEGLevel
alaErpRingPort1
alaErpRingPort2
alaErpRingPortIfIndex
alaErpRingState
alaErpRingVirtualChannel
alaErpRingRevertive
alaErpRingPortStatus
alaErpRingPortType
alaErpRingPortEthOAMEvent
alaErpRingPortRmepId
alaErpRingWaitToRestoreTimer
alaErpRingGuardTimer
alaErpRingLastStateChange
alaErpRingTimeToRevert
```

show erp protected-vlan

Displays the protected VLAN configuration for all ERP rings or for a specific ring.

show erp [ring *ring_id***] protected-vlan**

Syntax Definitions

ring_id	An existing ERP ring ID number. The valid range is 1- 2147483647.

Defaults

By default, the protected VLAN configuration is displayed for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Enter a ring ID to display the protected VLANs for a specific ring.
- The specified ring ID must already exist in the switch configuration.

Examples

```
-> show erp protected-vlan
Ring Id         : 1,
Protected VLAN  : 10 20 30-40
Ring Id         : 2,
Protected VLAN  : 50

-> show erp ring 3 protected-vlan
Ring Id         : 3,
Protected VLAN  : none
```

output definitions

Ring ID	The ERP ring ID number.
Protected VLAN	The VLAN IDs of the protected VLANs associated with the ring ID.

Release History

Release 6.6.2; command was introduced.
Release 6.7.2.R03; command deprecated.

Related Commands

show erp	Displays ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingId
alaErpRingVlanProtectedVid
```

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- 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 6450

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 already 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


-> show erp statistics ring 3
Legends: R-APS - Ring Automatic Protection Switching
         RPL   - Ring Protection Link

Ring-Id : 3
  Ring Port : 4/7
    Signal Fail PDUs
```

```
      Sent : 6,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 16,
      Recv : 14,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4351,
      Recv : 0,
      Drop : 0
    Invalid R-APS PDUs
      Recv : 0

  Ring Port : 6/1
    Signal Fail PDUs
      Sent : 6,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 13,
      Recv : 13,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4358,
      Recv : 0,
      Drop : 0
    Invalid R-APS PDUs
      Recv : 0


-> show erp statistics ring 1 port 1/15
Legends: R-APS - Ring Automatic Protection Switching
         RPL   - Ring Protection Link

Ring-Id : 1
  Ring Port : 1/15
    Signal Fail PDUs
      Sent : 3,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 37,
      Recv : 37,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4338,
      Recv : 0,
      Drop : 0
    Invalid R-APS PDUs
      Recv: 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 6.6.2; command was introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.
show erp protected-vlan	Displays the protected VLAN 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
```

18 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 (for example, a client equipment can drop BPDUs, or the STP protocol can be restricted to the network edge).

If a LBD frame which is originated from a device is received back by the same device, the port in which the LBD frame is received will go to shutdown state and the port at the other end where it is connected to will go to inactive state. When the two ports of a switch are connected to each other through a hub, either the port is shutdown or it is in normal state. On a linkagg port, LBD has to be enabled at port level.

When loopback occurs, a trap is sent and the event is logged. The port can manually be enabled again when the problem is resolved, or a Network Manager can define a recovery interval that automatically places the port into a “Normal” state after a defined period.

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
loopback-detection autorecovery-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 6450, 6350

Usage Guidelines

- LBD can be enabled globally and per port without any dependency but loopback-detection is 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 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 6.6.1; command was introduced.
Release 6.7.2; support for OmniSwitch 6350 added.

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 6450, 6350

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 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 6.6.1; command was introduced.
Release 6.7.2; support for OmniSwitch 6350 added.

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 6450, 6350

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 takes effect only after the timer is restarted.

Examples

```
-> loopback-detection transmission-timer 200
```

Release History

Release 6.6.1; command was introduced.
Release 6.7.2; support for OmniSwitch 6350 added.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information.

MIB Objects

```
alaLdbConfigTable
   alaLdbGLobalConfigTransmissionTimer
```

loopback-detection autorecovery-timer

Configures the LBD autorecovery timer on the switch. The autorecovery time is the time period in seconds that passes after which ports that were shut down through LBD are moved to normal state or inactive state, depending on the parameter that is set on the switch.

loopback-detection autorecovery-timer *seconds*

Syntax Definitions

seconds	The LBD autorecovery timer in seconds. The valid range is from 30 to 86400 seconds.

Defaults

parameter	default
seconds	300

Platforms Supported

OmniSwitch 6450, 6350
Release 6.7.2; support for OS6450.

Usage Guidelines

- If the autorecovery timer value is not configured, the default value of 300 seconds is assigned to the autorecovery period.
- The timer can be modified at any time. However, the new timer value takes effect only after the timer is restarted.

Examples

```
-> loopback-detection autorecovery-timer 300
```

Release History

Release 6.6.1; command was introduced.
Release 6.7.2; support for OmniSwitch 6350 added.

Related Commands

loopback-detection	Enables or disables LBD globally on the switch.
show loopback-detection	Displays LBD configuration information.

MIB Objects

```
alaLdbConfigTable
   alaLdbGLobalConfigAutorecoveryTimer
```

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 6450, 6350

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
Global LBD Auto-recovery Timer             : 300 sec

-> show loopback-detection port 1/1

Global LBD Status                          : Enabled
Global LBD Transmission Timer              : 200 sec
Global LBD Auto-recovery Timer             : 300 sec
Port LBD Status                            : Enabled
Port LBD State                             : Normal
```

output definitions

Global LBD Status	The status of LBD of the switch (**Enabled** or **Disabled**).
Global LBD Transmission Timer	Displays the time interval in seconds between LBD packet transmissions.
Global LBD Auto-recovery Timer	Displays the autorecovery time period in seconds. It is the time period that passes after which ports that were shut down through LBD are moved to normal state.

Release History

Release 6.6.1; command was introduced.
Release 6.7.2; support for OmniSwitch 6350 added.

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 are 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 6450, 6350

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
Global LBD Transmission Timer              : 300 sec
Port LBD Status                            : Enabled
Port LBD State                             : Normal
```

output definitions

Global LBD Status	The status of LBD of the switch (**Enabled** or **Disabled**).
Global LBD Transmission Timer	Displays the time interval in seconds between LBD packet transmissions.
Global LBD Auto-recovery Timer	Displays the autorecovery time period in seconds. It is the time period that passes after which ports that were shut down through LBD are moved to normal state.
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 6.6.1; command was introduced.
Release 6.7.2; support for OmniSwitch 6350 added.

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 6450, 6350

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 6.6.1; command was introduced.
Release 6.7.2; support for OmniSwitch 6350 added.

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
```

19 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.

This implementation of CPE Test Head supports unidirectional and bidirectional 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 CPE multi-test feature is supported on non-metro switches with metro license. The feature supports a stack containing up to eight switches.

Multi-stream test requires a free port. The port must not be used and not have 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 l2-saa** **test-oam start stop** **test-oam remote-sys-mac** **test-oam statistics flash-logging** **show test-oam** **show test-oam saa statistics** **clear test-oam statistics**
Multi-test	**test-oam group** **test-oam group tests** **test-oam feeder** **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 stop** **test-oam group remote-sys-mac** **show test-oam group** **show test-oam group statistics** **clear 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 6450

Usage Guidelines

- Use the **no** form of this command to remove the specified CPE test configuration.
- This command creates a new 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 6.6.2; command was introduced.

Related Commands

show test-oam	Displays the CPE test configuration and status.
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.

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 6450

Usage Guidelines

This command assigns the direction to the CPE test.

Examples

```
-> test-oam Test1 direction unidirectional
-> test-oam Test1 direction bidirectional
```

Release History

Release 6.6.3; command was introduced.
Release 6.6.5; **bidirectional** capability enabled.

Related Commands

show test-oam	Displays the CPE test configuration and status.
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.

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. The string can be of length 1to 32 characters.
src-string	This represents the local or transmitting device. The management IP address or DNS host name of the switch that will transmit test traffic. In case of bidirectional test this also identifies the analyzer device. The string can be of length 1to 32 characters.
dst-string	This represents the remote device. 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. For unidirectional test this represents the analyzer device. For bidirectional test this identifies the device on which the loopback mode must be active. The string can be of length 1to 32 characters.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The end point can be set as switch hostname or switch management IP address.
- 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.
- Multicast and broadcast address must not be configured for bidirectional 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 6.6.2; 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 6450

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 must be considered when test results are analyzed.
- This command automatically overwrites the port value previously configured for the specified CPE test.

Examples

```
-> test-oam Test1 port 1/2
```

Release History

Release 6.6.2; 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 6450

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 6.6.2; 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) or loopback test frames.

test-oam *string* **role {generator | analyzer | loopback}**

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.
loopback	Configures the switch as loopback.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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.
- 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
-> test-oam Test2 role loopback
```

Release History

Release 6.6.2; command was introduced.
Release 6.6.5; **loopback** mode supported.

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 1–3600 seconds
rate	The rate, in Kbps or Mbps, at which test traffic is generated. The minimum value allowed is 8 Kbps to line rate. The granularity of the transmit rate is 8 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	8 k
bytes	64 byte

Platforms Supported

OmniSwitch 6450

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.

Examples

```
-> test-oam Test1 duration 10 rate 8k packet-size 64
-> test-oam Test1 rate 8m
-> test-oam Test1 duration 10
-> test-oam Test1 packet-size 64
```

Release History

Release 6.6.2; 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* **priority** *priority* **drop-eligible {true | false}}]**
ether-type {*hex-num* | **ipv4 {src-ip** *src-ipv4* **dst-ip** *dst-ipv4* **[ttl** *ttl***] [tos** *tos***] [protocol {udp | tcp} {src-port** *src-port* **dst-port** *dst-port***}]}]} [data-pattern** *pattern***]**

Syntax Definitions

string	The name of an existing CPE test.
vlan-id	The VLAN ID of the frame.
priority	The priority value. The valid range is 0–7.
true	Sets the drop-eligible bit to true.
false	Sets the drop-eligible bit to false.
hex-num	The hexadecimal ethertype value. The valid range is 0x600–0xfffe.
src-ipv4	The source IP address for an IPv4 test frame.
dst-ipv4	The destination IP address for an IPv4 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.
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.
pattern	The data pattern present in the generated test frame. The valid range is 0x0000–0xffff.

Defaults

Parameter	Default
priority	7
drop-eligible	false
ttl	64
tos	0x0
pattern	0x0000

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Specify the Ether type in hexadecimal format to configure a Layer 2 test frame.
- Specify **ipv4** 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.
- 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 false 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 false 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
```

Release History

Release 6.6.2; command was introduced.

Related Commands

test-oam l2-saa	Start or stop the CPE test.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
alaTestOamEtherConfigTable
alaTestOamIpv4ConfigTable
```

test-oam l2-saa

Configures to run SAA tests in parallel with test streams.

test-oam *string* **l2-saa [priority** *vlan-priority***] [count** *num-pkts***] [interval** *inter-pkt-delay***] [continuous] [size** *size***] [drop-eligible {true | false}]**

no test-oam *string* **l2-saa**

Syntax Definitions

string	The name of an existing CPE test.
vlan-priority	Specify the internal priority of MAC ping and 802.1p value on the VLAN tag header.
num-pkts	The number of packets sent in one ping iteration. Valid range is 1 to 10.
inter-pkt-delay	The delay between packets sent during a ping iteration (milliseconds). Valid range is 100 to 1000, in multiples of 100.
continuous	Allows the SAA session to run continuously until the test-oam session ends.
size	The payload size to be used for MAC ping iteration. Must be within 1500 bytes.
drop-eligible	Specify the drop precedence of the MAC ping and the Canonical Format Indicator (CFI) bit on the VLAN tag header.

Defaults

Parameter	Default
vlan-priority	0
num-pkts	5
inter-pkt-delay	1000 ms
size	36 bytes
drop-eligible	false

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The L2-SAA test derives the source MAC, destination MAC, and the VLAN ID from the test OAM configuration of the individual test frames.
- The default L2-SAA configuration values will be applied if no optional parameters are configured.
- To run the L2-SAA session until the test-oam session ends, use the **continuous** parameter.
- Different SAA profiles can be configured for each individual test stream.

- Use the **no** form of this command to remove the L2-SAA configuration for the test.

Examples

```
-> test-oam test1 l2-saa priority 5 count 5 interval 1000 size 100 drop-eligible
false
-> test-oam test1 l2-saa continuous
-> no test-oam test1 l2-saa
```

Release History

Release 6.6.2; command was introduced.
Release 6.6.5; **l2-saa** option added.
Release 6.7.1; **continuous** option added.

Related Commands

test-oam	Configures the CPE test name and an optional description. The test name is used to identify and configure a CPE test profile.
show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamSaaConfigDropEligible
   alaTestOamSaaConfigPayloadSize
   alaTestOamSaaConfigNumPkts
   alaTestOamSaaConfigInterPktDelay
   alaTestOamSaaContinuous
```

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} [fetch-remote-stats]**

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.
fetch-remote-stats	Triggers the test at the remote device from the generator. The statistics are collected from the remote device and the test is stopped after receiving the test results.

Defaults

Parameter	Default
bytes	64

Platforms Supported

OmniSwitch 6450

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.
- Use the **fetch-remote-stats** parameter to collect the test statistics from the remote device. This parameter must be used to start the bidirectional test.

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
-> test-oam Test1 start fetch-remote-stats
-> test-oam "test2" port 1/2 start fetch-remote-stats
```

Release History

Release 6.6.2; command was introduced.
Release 6.6.5; **fetch-remote-stats** parameter added.

Related Commands

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	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestName
   alaTestOamConfigVlan
   alaTestOamConfigPort
   alaTestOamConfigGeneratorPacketSize
   alaTestOamConfigTestIdState
   alaTestOamConfigRemoteStatsFetch
```

test-oam remote-sys-mac

Configures the system MAC address of the remote device to receive test OAM messages.

test-oam *string* **remote-sys-mac** *string*

Syntax Definitions

string	The name of an existing CPE test.
remote-sys-mac	The system MAC address of the remote device.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use this command on the generator switch to set the system MAC address of the remote device to receive the test OAM messages.
- remote-sys-mac must be the primary CMM MAC address of the remote device. Use the **show cmm** command on the remote device to know the chassis MAC address of the device.
- remote-sys-mac is not applicable for analyzer or loopback.
- Configuring the Remote Sys MAC is mandatory for bidirectional test and optional for unidirectional test.

Examples

```
-> test-oam Test1 remote-sys-mac 00:e0:b1:7c:7a:fa
```

Release History

Release 6.6.5; command introduced.

Related Commands

show test-oam	Displays the CPE test configuration and status.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigRemoteSysMacAddress
```

test-oam statistics flash-logging

Enable or disable the option to save the statistics of the test on the file in the flash directory of the switch. The test information is appended at the end of the default text file (testoamActiveStats.txt) in the flash.

test-oam statistics flash-logging {enable | disable}

Syntax Definitions

N/A

Defaults

Parameter	Default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the **more** command to read the test results stored on the switch.

Examples

```
-> test-oam statistics flash-logging enable
-> test-oam statistics flash-logging disable
```

Release History

Release 6.6.5; command introduced.

Related Commands

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 saa statistics	Clears the statistics for all CPE tests or for a specific test name.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigStatsSave
```

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 6450

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: 1
Test-Id Port       Src-Mac        Dst-Mac         Vlan     Direction     Status         Remote-Sys-Mac
-------+-----+-----------------+-----------------+-----+--------------+-----------+----------------------
Test1   none  00:00:00:00:00:00  00:00:00:00:00:00 none  unidirectional  not-started  00:00:00:00:00:00
```

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.
Remote-Sys-Mac	The MAC address of the remote device configured through the **test-oam remote-sys-mac** command.

```
-> 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,
  Remote Sys MAC       : E8:E7:32:72:01:A4,
  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,
  Dei        : none,
  Ether Type : 0x8000,

-> 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,
  Remote Sys MAC       : E8:E7:32:72:01:A4,
  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        : 00:00:00:00:10.20.30.50,
      Destination Ip   : 00:00:00:00:10.30.40.60,
      Source Port      : 10,
      Destination Port : 20,
      Next Header      : tcp,
      Hop-Count        : 50,
      Traffic-Class    : 0xff
      Flow-Label       : 0x0
```

```
L2-SAA Configuration  :
  L2-SAA DE           : False,
  L2-SAA Payload Size : 64,
  L2-SAA Count        : 0,
  L2-SAA Interval     : 1000,
  L2-SAA Continuous    : yes
  L2-SAA Priority     : 0
```

output definitions

Source Endpoint	The host name for the source (generator) switch. Configured through the **test-oam direction** command.
Destination Endpoint	The host name for the destination (analyzer) switch. Configured through the **test-oam direction** 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.
Remote Sys MAC	The MAC address of the remote device configured through the **test-oam remote-sys-mac** 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 l2-saa** command.
Status	The operational status of the test (**running**, **ended**, **stopped**, or **not started**).
Frame Configuration	The test frame type (**ether** or **ipv4**) and associated parameter values. Configured through the **test-oam frame** command.
L2-SAA Configuration	Displays the L2 SAA configuration.

Release History

Release 6.6.2; command was introduced.
Release 6.6.5; **Remote Sys Mac** and **L2-SAA** details added.
Release 6.7.1; **L2-SAA Continuous** details added.

Related Commands

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.

MIB Objects

```
alaTestOamConfigTable
   alaTestOamConfigTestId
   alaTestOamConfigPort
   alaTestOamConfigFrameSrcMacAddress
   alaTestOamConfigFrameDstMacAddress
   alaTestOamConfigVlan
   alaTestOamConfigDirection
   alaTestOamConfigTestIdStatus
   alaTestOamConfigRemoteSysMacAddress

alaTestOamSaaConfigTable
   alaTestOamSaaConfigDropEligible
   alaTestOamSaaConfigPayloadSize
   alaTestOamSaaConfigNumPkts
   alaTestOamSaaConfigInterPktDelay
   alaTestOamSaaConfigVlanPriority
   alaTestOamSaaContinuous

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 6450

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      Remote-Stats  Throughput(Mbps)
--------+------------+------------+---------------+--------------+---------------
Test1    19017        19017         19017             19017         9.98


-> show test-oam statistics
Test-Id      TX-Ingress   TX-Egress    RX-Ingress Remote-Stats Throughput(Mbps)
------------+------------+------------+----------+------------+---------------
Test1        1200366      1200366          0       1200366      8
Test2          0             0          1200366    1200366      8
```

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.

output definitions

Remote-Stats	The number of test frames received by the analyzer and fetched by the generator device.
Throughput (Mbps)	Displays the traffic throughput of the test.

Release History

Release 6.6.2; command was introduced.
Release 6.6.5; **Remote-Stats** and **Throughput (Mbps)** fields added.

Related Commands

test-oam statistics flash-logging	Displays the CPE test configuration and status.
clear test-oam statistics	Clears CPE test statistics.

MIB Objects

```
alaTestOamStatsTable
   alaTestOamConfigTestId
   alaTestOamTxIngressCounter
   alaTestOamTxEgressCounter
   alaTestOamRxIngressCounter
   alaTestOamRemoteStatsCounter
   alaTestOamBandwidthThroughputStr
```

show test-oam saa statistics

Displays the SAA test statistics for all CPE tests or for a specific test name.

show test-oam [*string*] saa statistics

Syntax Definitions

string	The name of an existing CPE test.

Defaults

By default, statistics are displayed for all CPE tests.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the *string* parameter with this command to display SAA statistics for a specific CPE test.

Examples

```
-> show test-oam Test1 saa statistics

Test    Time of Last-Run       RTT    RTT    RTT   Jitter Jitter Jitter  Packets    Description
                               Min    Avg    Max    Min    Avg    Max   Sent Rcvd
-----+----------------------+-------+------+-----+------+------+------+----+------+-------------
Test1   2009-09-05,20:18:34.0  970    1067   1432    1    99      455    7    7      DEFAULT


-> show test-oam saa statistics
Test    Time of Last-Run       RTT    RTT    RTT   Jitter Jitter Jitter  Packets    Description
                               Min    Avg    Max    Min    Avg    Max   Sent Rcvd
-----+----------------------+------+----+-------+------+-------+-----+----+------+------------
Test1   2009-09-05,20:18:34.0  970    1067   1432    1    99      455    7    7      DEFAULT
Test2   2009-09-05,30:28:34.0  770    865    1432    2    99      255    7    7      DEFAULT
Test3   2009-09-05,40:38:34.0  570    967    1432    3    99      355    7    7      DEFAULT
Test4   2009-09-05,50:48:34.0  770    807    1432    1    99      255    7    7      DEFAULT
Test5   2009-09-06,20:18:34.0  640    867    1432    2    99      445    7    7      DEFAULT
Test6   2009-09-06,30:18:34.0  780    907    1432    3    99      255    7    7      DEFAULT
```

output definitions

Test	The CPE test name (ID).
Time of Last-Run	Displays the date and time on which the test was last run.
RTT Min	Displays the minimum round trip time.
RTT Avg	Displays the average round trip time.
RTT Max	Displays the maximum round trip time.
Jitter Min	Displays the minimum jitter value.
Jitter Avg	Displays the average jitter value.
Jitter Max	Displays the maximum jitter value.

output definitions

Packets Sent	Displays the number of packets sent during a single MAC ping.
Packets Rcvd	Displays the number of packets received during a single MAC ping.
Description	Displays the Test Description parameter value for each test

Release History

Release 6.6.5; command was introduced.

Related Commands

test-oam statistics flash-logging	Displays the CPE test configuration and status.
clear test-oam statistics	Clears CPE test statistics.

MIB Objects

```
alaTestOamSaaStatsTable
   alaTestOamConfigTestId
   alaTestOamSaaRunTime
   alaTestOamSaaPktsSent
   alaTestOamSaaPktsRcvd
   alaTestOamSaaMinRTT
   alaTestOamSaaAvgRTT
   alaTestOamSaaMaxRTT
   alaTestOamSaaMinJitter
   alaTestOamSaaAvgJitter
   alaTestOamSaaMaxJitter
```

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 6450

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 6.6.2; command was introduced.

Related Commands

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 saa statistics	Displays the SAA test statistics for all CPE tests or for a specific test name.

MIB Objects

```
alaTestOamStatsTable
   alaTestOamConfigTestId
   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 6450

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 6.6.3; 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. Use this command on both the generator and analyzer switch to determine test results.
show test-oam group	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 6450

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 6.6.3; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
show test-oam group	Displays the SAA statistics for all CPE test groups or for a specific CPE test group if mentioned.

MIB Objects

```
alaTestOamGroupFlowConfigTable
   alaTestOamConfigGroupId
   alaTestOamConfigTestId
   alaTestOamGroupFlowConfigRowStatus
```

test-oam feeder

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 6450

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.
- 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 6.6.3; 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

```
alaTestOamGlobalFeederPort
```

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 6450

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 6.6.3; 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 | loopback}**

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.
loopback	Configures the switch as loopback.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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
-> test-oam group Testgroup2 role loopback
```

Release History

Release 6.6.3; command was introduced.
Release 6.6.5; **loopback** mode supported.

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 6450

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 6.6.3; command was introduced.

Related Commands

test-oam group start stop	Starts the traffic test for the CPE test group on the configured port or the given port.
test-oam group remote-sys-mac	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 | bidirectional}]**

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 6450

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
-> test-oam group Testgroup2 direction bidirectional
```

Release History

Release 6.6.3; command was introduced.
Release 6.6.5; **bidirectional** capability enabled.

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 8 Kbps to line rate. The granularity of the transmit rate is 8 Kbps for 100 Mbps port and 2 Mbps for 1Gig ports.

Defaults

Parameter	Default
secs	5 secs
rate	8 k

Platforms Supported

OmniSwitch 6450

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 8m
-> test-oam group Testgroup1 duration 10 rate 8m
```

Release History

Release 6.6.3; 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 stop

Starts or stops the traffic test for the test-oam group on the configured port or the given port.

test-oam group *string* **{[port** *slot/port***] start | stop} [fetch-remote-stats]**

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.
stop	Disables the test.
fetch-remote-stats	Triggers the group test at the remote device from the generator. The statistics are collected during the test and the test is stopped after receiving the test results.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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.
- Use the fetch-remote-stats parameter to collect the test statistics from the remote device.

Examples

```
-> test-oam group Testgroup1 port 1/2 start
-> test-oam group Testgroup2 start
-> test-oam group Testgroup1 start fetch-remote-stats
-> test-oam group testgroup2 port 1/2 start fetch-remote-stats
-> test-oam group Testgroup1 stop
-> test-oam group Testgroup2 stop
```

Release History

Release 6.6.3; command was introduced.
Release 6.6.5; **fetch-remote-stats** parameter added.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
   alaTestOamGroupConfigState
   alaTestOamGroupConfigRemoteStatsFetchState
```

test-oam group remote-sys-mac

Configures the system MAC address of the remote device to receive test OAM messages.

test-oam group *string* **remote-sys-mac** *string*

Syntax Definitions

string	The name of an existing CPE test group.
remote-sys-mac	The system MAC address of the remote device.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use this command on the switch to set the system MAC address of the remote device to receive the test OAM messages.
- remote-sys-mac must be the primary CMM MAC address of the remote device.
- remote-sys-mac is not applicable for analyzer or loopback.

Examples

```
-> test-oam group Testgroup1 remote-sys-mac 00:e0:b1:7c:7a:fa
```

Release History

Release 6.6.5; command introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.

MIB Objects

```
alaTestOamGroupConfigTable
   alaTestOamGroupConfigRemoteSysMacAddress
```

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 6450

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 6.6.3; 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 6450

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: 2
Feeder Port      : none
Test-Group  Port  Duration     Rate    Nb of   Direction      Status        Remote-Sys-Mac
                   (secs)             Flows
----------+-----+----------+---------+-----+--------------+------------+--------------------
Testgroup1 none    5          -         2    unidirectional  not-started  00:00:00:00:00:00
Testgroup2 none    5          -         3    unidirectional  not-started  00:00:00:00:00:00
```

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.
Remote-Sys-Mac	The MAC address of the remote device configured through the **test-oam group remote-sys-mac** command.

```
-> show test-oam group Testgroup1
Legend: Port: * = Inactive port

TEST Parameters for Testgroup1:
  Source Endpoint         : SW1,
  Destination Endpoint    : SW2,
  Test Group Description  : first-testgroup,
  Direction               : bidirectional,
  Role                    : generator,
  Tx Rate                 : 10m,
  Duration                : 60 (secs),
  Port                    : 1/5,
  State                   : stop,
  Status                  : not-started,
  Remote Sys MAC          : E8:E7:32:32:A6:EE
    Flow 1:
      Test Name           : test1,
      Vlan                : 1001,
      Tx Rate             : 10m,
      Source MAC          : 00:11:22:12:44:55,
      Destination MAC     : 00:22:33:12:55:66,
      Remote Sys MAC      : E8:E7:32:32:A6:EE,
      Frame Size          : 64,
      L2-SAA DE           : False,
      L2-SAA Payload Size : 64,
      L2-SAA Count        : 5,
      L2-SAA Interval     : 1000,
      L2-SAA Priority     : 0
      L2-SAA Continuous   : no
    Flow 2:
      Test Name           : test2,
      Vlan                : 1001,
      Tx Rate             : 10m,
      Source MAC          : 00:11:22:13:44:55,
      Destination MAC     : 00:22:33:13:55:66,
      Remote Sys MAC      : E8:E7:32:32:A6:EE,
      Frame Size          : 100,
      L2-SAA DE           : True,
      L2-SAA Payload Size : 120,
      L2-SAA Count        : 0,
      L2-SAA Interval     : 900,
      L2-SAA Priority     : 6
      L2-SAA Continuous   : yes
    Flow 3:
      Test Name           : test3,
      Vlan                : 1001,
      Tx Rate             : 10m,
      Source MAC          : 00:11:22:14:44:55,
      Destination MAC     : 00:22:33:14:55:66,
      Remote Sys MAC      : E8:E7:32:32:A6:EE,
      Frame Size          : 100,
      L2-SAA DE           : True,
      L2-SAA Payload Size : 120,
      L2-SAA Count        : 0,
      L2-SAA Interval     : 900,
      L2-SAA Priority     : 6
      L2-SAA Continuous   : yes
    Flow 4:
      Test Name           : test4,
```

```
Vlan                : 1001,
Tx Rate             : 10m,
Source MAC          : 00:11:22:15:44:55,
Destination MAC     : 00:22:33:15:55:66,
Remote Sys MAC      : E8:E7:32:32:A6:EE,
Frame Size          : 100
L2-SAA DE           : True,
L2-SAA Payload Size : 120,
L2-SAA Count        : 0,
L2-SAA Interval     : 900,
L2-SAA Priority     : 6
L2-SAA Continuous   : yes
```

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.
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.
Remote Sys Mac	The MAC address of the remote device configured through the **test-oam group remote-sys-mac** 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.
L2-SAA Count	Specifies the number of packets sent in one MAC ping iteration.
L2-SAA Interval	Specifies the delay between two consecutive packets transmitted during a MAC ping iteration.
L2-SAA DE	Specifies if the drop enable bit value is used.
L2-SAA Payload Size	Specifies the size of the MAC ping payload used for the MAC ping operation.
L2-SAA Priority	Specifies the priority value set for the L2 SAA frames.
L2-SAA Continuous	Specifies the SAA session will run continuously until the test-oam session ends.

Release History

Release 6.6.3; command was introduced.
Release 6.6.5; **Remote Sys Mac** and **L2-SAA** details added.
Release 6.7.1; **L2-SAA continuous** details added.

Related Commands

show test-oam group	Displays the statistics for all CPE test groups or for a specific CPE test group.

MIB Objects

```
alaTestOamGloabalFeederPort
alaTestOamGroupConfigTable
alaTestOamGroupConfigRowStatus
   alaTestOamConfigGroupId
   alaTestOamGroupConfigPort
   alaTestOamGroupConfigDuration
   alaTestOamGroupConfigGeneratorBandwidth
   alaTestOamGroupConfigFlowCount
   alaTestOamGroupConfigDirection
   alaTestOamGroupConfigStatus
   alaTestOamGroupConfigRemoteStatsFetchState
   alaTestOamGroupConfigRemoteSysMacAddress
alaTestOamGroupConfigTable
     alaTestOamConfigGroupId
     alaTestOamGroupConfigSourceEndpoint
     alaTestOamGroupConfigDestinationEndpoint
     alaTestOamConfigGroupDescription
     alaTestOamGroupConfigDirection
     alaTestOamGroupConfigRole
     alaTestOamGroupConfigGeneratorBandwidth
     alaTestOamGroupConfigDuration
     alaTestOamGroupConfigPort
     alaTestOamGroupConfigState
     alaTestOamGroupConfigStatus
    alaTestOamGroupConfigStatsClear

  alaTestOamGroupFlowConfigTable
    alaTestOamConfigTestId
    alaTestOamGroupFlowVlan
    alaTestOamConfigGroupId
    alaTestOamGroupFlowGeneratorBandwidth
    alaTestOamGroupFlowFrameSrcMacAddress
    alaTestOamGroupFlowFrameDstMacAddress
    alaTestOamGroupFlowGeneratorPacketSize
```

show test-oam group saa statistics

Displays the SAA test statistics for all CPE test groups or for a specific test name.

show test-oam group [*string***] saa statistics**

Syntax Definitions

string	The name of an existing CPE test group.

Defaults

By default, statistics are displayed for all CPE test group.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the *string* parameter with this command to display SAA statistics for a specific CPE test group.

Examples

```
-> show test-oam group Test1 saa statistics

Test-group Flow Time of Last-Run       RTT    RTT    RTT   Jitter Jitter Jitter  Packets    Description
                                       Min    Avg    Max    Min    Avg    Max   Sent Rcvd
---------+-----+--------------------+-------+------+-----+------+------+------+----+------+-------------
Test1     flow1 2009-09-05,20:18:34.0  970    1067   1432    1    99      455    7    7      DEFAULT


-> show test-oam group saa statistics

Latest Record:
Test-group Flow Time of Last-Run       RTT    RTT    RTT   Jitter Jitter Jitter  Packets    Description
                                       Min    Avg    Max    Min    Avg    Max   Sent Rcvd
---------+-----+--------------------+------+-----+-------+-----+------+-----+-----+------+------------
Test1     flow1 2009-09-05,20:18:34.0  970    1067   1432    1    99      455    7    7      DEFAULT
Test2     flow2 2009-09-05,30:28:34.0  770    865    1432    2    99      255    7    7      DEFAULT
Test3     flow3 2009-09-05,40:38:34.0  570    967    1432    3    99      355    7    7      DEFAULT
Test4     flow4 2009-09-05,50:48:34.0  770    807    1432    1    99      255    7    7      DEFAULT
Test5     flow5 2009-09-06,20:18:34.0  640    867    1432    2    99      445    7    7      DEFAULT
Test6     flow6 2009-09-06,30:18:34.0  780    907    1432    3    99      255    7    7      DEFAULT
```

output definitions

Test-group	The CPE test group name (ID).
Flow	Displays the flow identifier for the test.
Time of Last-Run	Displays the date and time on which the test was last run.
RTT Min	Displays the minimum round trip time.
RTT Avg	Displays the average round trip time.
RTT Max	Displays the maximum round trip time.
Jitter Min	Displays the minimum jitter value.

output definitions

Jitter Avg	Displays the average jitter value.
Jitter Max	Displays the maximum jitter value.
Packets Sent	Displays the number of packets sent during a single MAC ping.
Packets Rcvd	Displays the number of packets received during a single MAC ping.
Description	Displays the description for each provided by the user during the test creation. By default it is displayed as “DEFAULT”.

Release History

Release 6.6.5; command was introduced.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
clear test-oam group statistics	This clears the statistics of the CPE test group.

MIB Objects

```
alaTestOamGroupFlowSaaStats
   alaTestOamConfigGroupId
   alaTestOamConfigTestId
   alaTestOamGroupFlowSaaStatsEntry
   alaTestOamGroupFlowSaaRunTime
   alaTestOamGroupFlowSaaPktsSent
   alaTestOamGroupFlowSaaPktsRcvd
   alaTestOamGroupFlowSaaRunTime
   alaTestOamGroupFlowSaaMinRTT
   alaTestOamGroupFlowSaaAvgRTT
   alaTestOamGroupFlowSaaMaxRTT
   alaTestOamGroupFlowSaaMinJitter
   alaTestOamGroupFlowSaaAvgJitter
   alaTestOamGroupFlowSaaMaxJitter
```

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 6450

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   Remote-Stats
-----------+--------+-------------+---------------+------------+-----------
TestGroup4   flow1     19017         19017             0           19017
TestGroup4   flow2     19017         19017             0           19017

-> show test-oam group statistics
Test-Group Flow   TX-Ingress   TX-Egress    RX-Ingress    Remote-Stats  Throughput(Mbps)
---------+------+------------+------------+-------------+-------------+---------------
Testgroup1 test1   20163463     17205475            0      17205475          172.05
Testgroup1 test2   20720137     17680541            0      17680541          176.81
Testgroup1 test3   20709603     17668483            0      17668483          176.68
Testgroup1 test4   20698156     17656987            0      17656987          176.57
Testgroup2 test1   20163463     17205475            0      17205475          172.05
Testgroup2 test2   20720137     17680541            0      17680541          176.81
Testgroup2 test3   20709603     17668483            0      17668483          176.68
Testgroup2 test4   20698156     17656987            0      17656987          176.57
```

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.

output definitions

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.
Remote-Stats	The number of test frames received by the analyzer and fetched by the generator device.
Throughput(Mbps)	Displays the traffic throughput of the test.

Release History

Release 6.6.3; command was introduced.
Release 6.6.5; **Remote-Stats** and **Throughput (Mbps)** fields added.

Related Commands

show test-oam group	Displays the configuration and status of the CPE test groups.
test-oam group remote-sys-mac	Clears the statistics of the CPE test group.

MIB Objects

```
alaTestOamGroupFlowStatsTable
   alaTestOamConfigGroupId
   alaTestOamConfigTestId
   alaTestOamGroupFlowTxIngressCounter
   alaTestOamGroupFlowTxEgressCounter
   alaTestOamGroupFlowRxIngressCounter
   alaTestOamGroupFlowRemoteStatsCounter
   alaTestOamGroupBandwidthThroughputStr
```

20 Source Learning Commands

Source Learning is responsible for creating, updating, and deleting source and destination MAC Address entries in the MAC Address Table. This chapter includes descriptions of Source Learning commands used to create or delete static MAC addresses, define the aging time value for static and dynamically learned MAC addresses, and display MAC Address Table entries and statistics.

MIB information for Source Learning commands is as follows:

Filename: AlcatelInd1MacAddress.mib
Module: ALCATEL-IND1-MAC-ADDRESS-MIB

A summary of the available commands is listed here:

mac-address-table
mac-address-table static-multicast
mac-address-table aging-time
source-learning
hash-control chain-length
show mac-address-table
show mac-address-table static-multicast
show mac-address-table count
show mac-address-table aging-time
show source-learning
show hash-control chain-length

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 (for example, 00:00:39:59:f1:0c).
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).
link_agg	Enter a link aggregate ID number (0–31). See Chapter 12, "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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove a MAC address from the Source Learning MAC Address Table.
- When **no mac-address-table** command is used, the 802.1x users entry will continue to be maintained in mac-address-table and 802.1x table and there will not be impact on 802.1x users traffic.
- 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 20-7) to set the aging time value for all static and dynamically learned MAC addresses. This is the value applied to static MAC addresses defined using the **mac-address-table timeout** form of this command.

Examples

```
-> mac-address-table permanent 00:00:39:59:f1:0c 4/2 355
-> no mac-address-table
-> no mac-address-table 5/1 755
-> no mac-address-table permanent
```

Release History

Release 6.6.1; 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

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblProtocol
```

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 (for example, 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 12, "Link Aggregation Commands."
vid	VLAN ID number (1–4094).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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, and so on, 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 includes 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 6.6.1; command was introduced.

Related Commands

show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table static-multicast	Displays a list of static multicast MAC addresses that are configured in the Source Learning MAC Address Table.
show mac-address-table count	Displays Source Learning MAC Address Table statistics.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
```

```
slMacAddressGblProtocol
```

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—634.

Defaults

By default, the aging time is set to 300 seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 20-2) to configure a static MAC address, then the aging time value is not applied to the static MAC address.
- The MAC address table aging time is also used as the timeout value for the Address Resolution Protocol (ARP) table. This timeout value determines how long the switch retains dynamically learned ARP table entries.

Examples

```
-> mac-address-table aging-time 1200
-> no mac-address-table aging-time
```

Release History

Release 6.6.1; command was introduced.

Related Commands

mac-address-table	Configures a static destination Unicast MAC address for a VLAN bridge.
show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table count	Displays Source Learning MAC Address Table statistics.
show mac-address-table aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
slMacAddressAgingTable
   slMacAgingValue
```

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 (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, 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 6450

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 the 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 6.6.1; command introduced.
Release 6.7.2; Support for non-metro switches.

Related Commands

show source-learning	Displays Source Learning status of each port or linkagg ports on a switch.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacLearningControlTable
   slMacLearningControlEntry
   slMacLearningControlStatus
```

hash-control chain-length

Configures the hash chain length in the hardware. Depending upon this configuration, the hashing bucket size for the hardware table will be decided.

hash-control chain-length default
hash-control chain-length extend

Syntax Definitions

default	If configured, Hash Chain Length will be set to 4.
extend	If configured, Hash Chain Length will be set to 8.

Defaults

By default, hash control chain length is set as default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to change the hash chain length from **default** to **extend** mode and vice-versa.
- After using this command, save the configurations using **write memory** command and reload the switch to reflect the hash length changes in the switch.

Examples

```
-> hash-control chain-length default

-> hash-control chain-length extend
   INFO:Changed hash chain length for FDB table will take effect if command is
   saved on next switch reboot
```

Release History

Release 6.7.2; command introduced.

Related Commands

show hash-control chain-length Displays the configured value for the depth of the hashing bucket.

MIB Objects

```
alaChasFdbHashChainLength
```

show hash-control chain-length

Displays the configured value for the depth of the hashing bucket.

show hash-control chain-length

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The * symbol displayed in the show output (FDB Hash Chain Length = EXTEND*) indicates that the configured hash chain length will be applied only after reloading the switch.
- If any modification in hash chain length is made by the user, it is important to reload/reboot of the switch/stack. Only the configured value will be displayed for SNMP and Webview. Any configuration changes made with respect to hash chain length in CLI/SNMP/Webview requires switch reboot to get the configuration changes applied in the switch.
- Without performing a reboot (after change in hash length), actions like inserting a new NI or doing takeover should not be done.

Examples

```
-> show hash-control chain-length
FDB Hash Chain Length = DEFAULT

-> show hash-control chain-length
(*=new hash chain length config will be applied after reboot)
FDB Hash Chain Length = EXTEND*
```

Release History

Release 6.7.2; command introduced.

Related Commands

hash-control chain-length	Configures the hash chain length in the hardware. Depending upon this configuration, the hashing bucket size for the hardware table will be decided..

MIB Objects

```
alaChasFdbHashChainLength
```

show mac-address-table

Displays Source Learning MAC Address Table information.

show mac-address-table [permanent | learned] [*mac_address***] [slot** *slot* **|** *slot/port***] [linkagg** *link_agg***] [***vid* **|** *vid1-vid2***]**

Syntax Definitions

permanent	Display static MAC addresses with a permanent status.
learned	Display dynamically learned MAC addresses.
mac_address	Enter a MAC Address (for example, 00:00:39:59:f1:0c).
slot	Enter the slot number for a module to specify that the command has to include all ports on that module (for example, 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 (for example, 3/1 specifies port 1 on slot 3).
link_agg	Enter a link aggregate ID number (0–31). See Chapter 12, "Link Aggregation Commands."
vid	A single VLAN ID number (1–4094).
vid1-vid2	A contiguous range of VLAN ID numbers (for example, 5-10).

Defaults

By default, information is displayed for all MAC addresses contained in the table.

Platforms Supported

OmniSwitch 6450, 6350

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

   Vlan      Mac Address          Type       Protocol    Operation    Interface
  ------+------------------+-------------+-----------+------------+-----------
     1   00:00:00:00:00:01     learned        0800        bridging      8/ 1
     1   00:d0:95:6a:73:9a     learned        aaaa0003    bridging     10/23
Total number of Valid MAC addresses above = 2


-> show mac-address-table 10-15
Legend: Mac Address: * = address not valid

   Vlan      Mac Address          Type       Protocol    Operation    Interface
  ------+------------------+-------------+-----------+------------+-----------
    10   00:00:00:00:00:01     learned        0800        bridging      1/2
    10   00:d0:95:6a:73:9a     learned        aaaa0003    bridging      1/2
    11   00:d0:95:a3:e0:0d     learned            ---     bridging      1/3
    11   00:d0:95:a3:e5:09     learned            ---     bridging      1/3
    11   00:d0:95:a3:e7:75     learned            ---     bridging      1/4
    12   00:d0:95:a3:ed:f7     learned            ---     bridging      2/1
    12   00:d0:95:a8:2a:b6     learned            ---     bridging      2/1
    12   00:d0:95:ad:e3:cc     learned            ---     bridging      2/1
    13   00:d0:95:ae:3b:f6     learned            ---     bridging      2/8
    13   00:d0:95:b2:3d:fa     learned            ---     bridging      2/8
 Total number of Valid MAC addresses above = 14
```

output definitions

VLAN	Vlan ID number associated with the MAC address and slot/port.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status: **learned or permanent**. Use the **mac-address-table** command on page 20-2 to configure the management status for a static MAC address.
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) or **filtering**. Use the **mac-address-table** command on page 20-2 to configure the disposition for a static MAC address.
Interface	The slot number for the module and the physical port number on that module that is associated with the static or dynamically learned MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29).

Release History

Release 6.6.1; command was introduced.

Related Commands

show mac-address-table count	Displays Source Learning MAC Address Table statistics.
show mac-address-table aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblProtocol
```

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 (for example, 01:00:39:59:f1:0c).
slot	Enter the slot number for a module to specify that the command has to include all ports on that module (for example, 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 (for example, 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	A contiguous range of VLAN ID numbers (for example, 5-10).

Defaults

By default, information is displayed for all static multicast MAC addresses contained in the MAC address table.

Platforms Supported

OmniSwitch 6450, 6350

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

   Vlan      Mac Address          Type       Protocol    Operation    Interface
  ------+------------------+-------------+-----------+------------+-----------
     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

   Vlan      Mac Address          Type       Protocol    Operation    Interface
  ------+------------------+-------------+-----------+------------+-----------
 *   1   01:00:00:00:00:01     static-mcast        0      bridging      1/1
    24   00:d0:95:e4:cf:5a     learned            ---     bridging      1/2
    24   00:d0:95:e5:af:52     learned            ---     bridging      1/2
    24   00:e0:4c:bc:ce:a1     learned            ---     bridging      1/2
     1   01:00:00:00:00:02     static-mcast       ---     bridging      2/6
     1   00:d0:95:e2:77:38     learned            ---     bridging      3/19
Total number of Valid MAC addresses above = 5
```

output definitions

VLAN	Vlan ID number associated with the static multicast address.
Mac Address	The multicast MAC address that is statically assigned to the VLAN and slot/port.
Type	Indicates the MAC address is a static multicast (**static-mcast**) address. This type of address is configured through the **mac-address-table static-multicast** command.
Protocol	Protocol type for the MAC address entry.
Operation	The disposition of the MAC address: **bridging** (default) or **filtering**. Note that this value is always set to **bridging** for static multicast addresses.
Interface	The slot number for the module and the physical port number on that module that is associated with the static multicast MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29).

Release History

Release 6.6.1; command was introduced.

Related Commands

show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table count	Displays Source Learning MAC Address Table statistics.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacAddressGblManagement
   slMacAddressGblDisposition
   slMacAddressGblRowStatus
   slMacAddressGblProtocol
```

show mac-address-table count

Displays Source Learning MAC Address Table statistics.

show mac-address-table count [*mac_address***] [slot** *slot* | *slot/port***] [linkagg** *link_agg***] [***vid* | *vid1-vid2***]**

Syntax Definitions

mac_address	MAC Address (for example, 00:00:39:59:f1:0c).
slot | *slot/port*	Slot number for the module or the slot number and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
link_agg	Enter a link aggregate ID number (0–31). See Chapter 12, "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 6450, 6350

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
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
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 6.6.1; command was introduced.

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.

MIB Objects

N/A

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 6450, 6350

Usage Guidelines

- The MAC Address Table aging time applies to static MAC addresses that were defined using the **time-out** parameter (see page 20-2) and to dynamically learned MAC addresses.
- Note that the aging time is the same for all VLANs because it is not configurable on a per-VLAN basis. The aging time value on this platform is a global parameter that applies to all VLANs.

Examples

```
-> show mac-address-table aging-time
Mac Address Aging Time (seconds) = 300
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show mac-address-table	Displays Source Learning MAC Address Table information.
show mac-address-table count	Displays Source Learning MAC Address Table statistics.

MIB Objects

```
slMacAddressAgingTable
   slMacAgingValue
```

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 (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, 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 6450

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 (for example, 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 6.6.1; command was 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.

MIB Objects

```
alaSlMacAddressGlobalTable
   slMacLearningControlTable
   slMacLearningControlEntry
   slMacLearningControlStatus
```

21 PPPoE Intermediate Agent

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 {port | linkagg}
pppoe-ia {trust | 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 {port | linkagg}
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

Enable or disable PPPoE-IA globally on the switch.

pppoe-ia {enable | disable}

Syntax Definitions

enable	Enable PPPoE-IA.
disable	Disable PPPoE-IA.

Defaults

By default, PPPoE-IA is disabled globally on the switch.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

All PPPoE-IA parameters are configurable irrespective of the global status of PPPoE-IA.

Examples

```
-> pppoe-ia enable
-> pppoe-ia disable
```

Release History

Release 6.6.3; command introduced.

Related Commands

pppoe-ia {port | linkagg}	Enable or disable PPPoE-IA on a port or a link aggregate port.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
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.
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.
show pppoe-ia {port | linkagg}	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

```
alaPPPoEIAGlobalStatus
```

pppoe-ia {port | linkagg}

Enable or disable PPPoE-IA on a port or a link aggregate port. Link aggregate can be either static or dynamic.

pppoe-ia {port *slot*/*port*[-*port2*] **| linkagg** *agg_num***} {enable | disable}**

Syntax Definitions

slot	The slot number for the module (for example, 3 specifies slot 3)
port	Port number of the interface to be configured (for example, 3/1 specifies port 1 on slot 3)
port2	Last port number in a range of ports to be configured (for example, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
linkagg *agg_num*	The link aggregate identification number.
enable	Enable PPPoE-IA on a port.
disable	Disable PPPoE-IA on a port.

Defaults

By default, PPPoE-IA is disabled on all ports.

Platforms Supported

OmniSwitch 6450

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 port 1/1 enable
-> pppoe-ia port 2/4 disable
-> pppoe-ia linkagg 1 enable
```

Release History

Release 6.6.3; 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.
show pppoe-ia {port | linkagg}	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
```

pppoe-ia {trust | client}

Configures a port or a link aggregate port as trusted or client port for PPPoE-IA.

A trust 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_num***} {trust | client}**

Syntax Definitions

slot	The slot number for the module (for example, 3 specifies slot 3)
port	Port number of the interface to be configured (for example, 3/1 specifies port 1 on slot 3)
port2	Last port number in a range of ports to be configured (for example, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
linkagg *agg_num*	Specifies the link aggregate identification number.
trust	Specifies the mode of the port as trust.
client	Specifies the mode of the port as client.

Defaults

By default, all ports are client ports.

Platforms Supported

OmniSwitch 6450

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 port 1/2-6 client
-> pppoe-ia linkagg 7 trust
-> pppoe-ia linkagg 0 client
```

Release History

Release 6.6.3; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {port | linkagg}	Enable or disable PPPoE-IA on a port or a link aggregate port.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	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 6450

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 6.6.3; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {port | linkagg}	Enable or disable PPPoE-IA on a port or a link aggregate port.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
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.
show pppoe-ia {port | linkagg}	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

```
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 [atm] 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 used for the Ethernet parameter.
atm	When the PPPoE-IA Circuit-ID format is configured as “default atm” the Circuit-ID encoding happens for “ATM” (Asynchronous Transfer Mode) parameter.
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.

Defaults

parameter	default
char	**:**

By default, “:” (colon) is used as the delimiter.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Circuit-ID identification is configurable only globally and cannot be configured on a per-port or per-VLAN basis.

- To configure ethernet default parameter, use “default” in the CLI command.
- To configure default parameter as “atm”, use “default ATM” in the CLI command.
- When the PPPoE-IA Circuit-ID format is configured as “default atm” the Circuit-ID encoding happens for “ATM” (Asynchronous Transfer Mode) parameter.
- 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 “:”. The available delimiters are: “:” (colon), “|” (pipe), “/” (forward slash), “\” (backward slash), “-” (hyphen), “'_” (underscore), “ ” (space), “#” (hash), “.” (full stop), “,” (comma), “;” (semicolon).
- 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 is 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 default
-> pppoe-ia circuit-id default atm
-> 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 6.6.3; command introduced.
Release 6.6.4; “atm” keyword was added.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	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

```
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 6450

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 6.6.3; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
show pppoe-ia configuration	Displays the global configuration for PPPoE-IA.
show pppoe-ia {port | linkagg}	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

```
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_num***]**

Syntax Definitions

slot	The slot number for the module (for example, 3 specifies slot 3)
port	Port number of the interface to be configured (for example, 3/1 specifies port 1 on slot 3)
port2	Last port number in a range of ports to be configured (for example, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
linkagg *agg_num*	Specifies the link aggregate identification number.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> clear pppoe-ia statistics
-> clear pppoe-ia statistics linkagg 13
```

Release History

Release 6.6.3; command introduced.

Related Commands

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.
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

```
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 6450

Usage Guidelines

- If the Circuit-ID is configured with “default” parameter, then the Circuit-ID format will display as “ethernet”.
- If the Circuit-ID is configured with “default atm” parameter, then the Circuit-ID format will display as “atm”.

Examples

```
Default Configuration
-> pppoe-ia circuit-id default
-> 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       : ethernet,
  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
```

```
-> pppoe-ia circuit-id default atm
-> show pppoe-ia configuration
Status                     : enabled,
Access Node Identifier
  Access-node-id Format    : base-mac,
  Access-node-id String    : 00:d0:95:ee:fb:02,
Circuit Identifier
  Circuit-Id Format        : atm,
  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
```

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 6.6.3; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
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.
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

```
alaPPPoEIAGlobalStatus
   alaPPPoEIAGlobalAccessNodeIDFormatType
   alaPPPoEIAGlobalAccessNodeIDStringValue
   alaPPPoEIAGlobalCircuitIDFormatType
   alaPPPoEIAGlobalCircuitIDField1
   alaPPPoEIAGlobalCircuitIDField1StrVal
   alaPPPoEIAGlobalCircuitIDField2
   alaPPPoEIAGlobalCircuitIDField2StrVal
   alaPPPoEIAGlobalCircuitIDField3
   alaPPPoEIAGlobalCircuitIDField3StrVal
   alaPPPoEIAGlobalCircuitIDField4
   alaPPPoEIAGlobalCircuitIDField4StrVal
   alaPPPoEIAGlobalCircuitIDField5
   alaPPPoEIAGlobalCircuitIDField5StrVal
   alaPPPoEIAGlobalCircuitIDDelimiter
   alaPPPoEIAGlobalRemoteIDFormatType
   alaPPPoEIAGlobalRemoteIDStringValue
   alaPPPoEIAGlobalClearStats
```

show pppoe-ia {port | linkagg}

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_num***} [enabled | disabled | trusted | client]**

Syntax Definitions

slot	The slot number for the module (for example, 3 specifies slot 3)
port	Port number of the interface to be configured (for example, 3/1 specifies port 1 on slot 3)
port2	Last port number in a range of ports to be configured (for example, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
linkagg *agg_num*	Specifies the link aggregate identification number.
enabled	PPPoE-IA enabled port.
disable	PPPoE-IA disabled port.
trust	Port configured as trust.
client	Port configured as client.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

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 trust or client port for PPPoE-IA.

Release History

Release 6.6.3; command introduced.

Related Commands

pppoe-ia	Enable or disable PPPoE-IA globally on the switch.
pppoe-ia {trust | client}	Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
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.
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

```
alaPPPoEIAGlobalStatus
alaPPPoEIAGlobalAccessNodeIDFormatType
alaPPPoEIAGlobalAccessNodeIDStringValue
alaPPPoEIAGlobalCircuitIDFormatType
alaPPPoEIAGlobalCircuitIDField1
alaPPPoEIAGlobalCircuitIDField1StrVal
alaPPPoEIAGlobalCircuitIDField2
alaPPPoEIAGlobalCircuitIDField2StrVal
alaPPPoEIAGlobalCircuitIDField3
```

```
alaPPPoEIAGlobalCircuitIDField3StrVal
alaPPPoEIAGlobalCircuitIDField4
alaPPPoEIAGlobalCircuitIDField4StrVal
alaPPPoEIAGlobalCircuitIDField5
alaPPPoEIAGlobalCircuitIDField5StrVal
alaPPPoEIAGlobalCircuitIDDelimiter
alaPPPoEIAGlobalRemoteIDFormatType
alaPPPoEIAGlobalRemoteIDStringValue
```

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 {port {*slot*/*port*[*-port2*] **| linkagg** *agg_num***} statistics**

Syntax Definitions

slot	The slot number for the module (for example, 3 specifies slot 3)
port	Port number of the interface to be configured (for example, 3/1 specifies port 1 on slot 3)
port2	Last port number in a range of ports to be configured (for example, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
linkagg *agg_num*	Specifies the link aggregate identification number.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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.
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 6.6.3; command introduced.

Related Commands

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.
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
```

22 Learned Port Security Commands

Learned Port Security (LPS) provides a mechanism for controlling network device communication on one or more switch ports. LPS does not support link aggregate and tagged (trunked) link aggregate ports. LPS can be used to control source MAC address learning.

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 during 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 LPS on the switch ports. When LPS is enabled, only devices that have a source MAC address that complies with LPS restrictions are learned on the ports.

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.
disable	Disables LPS on the specified port.
locked	Disables source learning on the specified LPS port.
chassis convert-to-static	Converts the learned bridge MAC address on all the LPS ports into static MAC address. This does not apply to filtered MAC addresses.
chassis disable	Disables all LPS-eligible ports on the chassis.

Defaults

By default, LPS is disabled on all switch ports.

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

Platforms Supported

OmniSwitch 6450, 6350

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 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 MAC addresses 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.
- When **admin-status** is disabled, all filtered MAC addresses on the port are removed and all bridged and static MAC addresses are retained in "forwarding" state. The LPS static MAC configuration is retained. Source learning is set for the port and all new MAC addresses are learned. The port-security configuration is allowed but not applied, but configuration of LPS static MAC is not allowed.

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 6.6.1; command introduced.
Release 6.6.3; **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 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 ports.

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.

Configures all the options for learning window to default when the shut down time is zero and default option is applied.

port-security shutdown *num* **[no-aging {enable | disable}] [convert-to-static {enable | disable}] [boot-up {enable | disable}] [mac-move {enable | disable}] [learn-as-static {enable | disable}]**

port-security shutdown 0 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.
mac-move enable	Enables the movement of pseudo-static or static MAC when learning window is enabled.
mac-move disable	Disables the movement of pseudo-static or static MAC when learning window is enabled or disabled.
learn-as-static enable	Enables LAS functionality.This option is used for learning a MAC as static when learning window is active.
learn-as-static disable	Disables LAS functionality without removing LPS configuration. Learning is unrestricted.
default	All options for learning window are set to their default values.

Defaults

By default, the LPS source learning time limit is not set for the switch.

parameter	default
convert-to-static	**disable**
no-aging	**disable**
boot-up	**enable**
learn-as-static	**disable**
mac-move	**disable**

Platforms Supported

OmniSwitch 6450, 6350

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 on the switch). 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 learned 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.
- When **learn-as-static** is enabled, during learning window the MAC is learned as pseudo-static and automatically set to a static LPS even if convert-to-static is enabled or disabled.
  For a duplicate MAC learned during the learning window, MAC movement is allowed when both **learn-as-static** and **mac-move** are enabled.

- The **no-aging** option must be enabled before enabling **learn-as-static**.
  - If **no-aging** is disabled, then, enabling **learn-as-static** displays an error message:
  `“Cannot enable learn as static option as no-aging option is not enabled".`
  - If **learn-as-static** is enabled, then, disabling **no-aging** option displays an error message:
  `"Cannot disable no-aging as learn-as-static or mac-move still enabled"`

- When **mac-move** is enabled, during learning window:
  - A pseudo-static MAC is allowed to move to a new port and the MAC is removed from the old port.
  - In case of Static MACs, the same MACs are learned as static on new port and are marked as duplicate on the old port.
  - When learning window expires, pseudo static MACs move as a filter to the new port and flushed at old port.
  - In case of static MACs, the MAC is learned as a filter at new port and duplicate at old port.

- The **no-aging** option must be enabled before enabling **mac-move.**
  - If **no-aging** is disabled, then, enabling **mac-move** displays an error message:
  `ERROR: Cannot enable learn as static option as no-aging option is not enabled.`
  - If **mac-move** is disabled, then, enabling **no-aging** displays an error message:
  `ERROR: Cannot disable no-aging as learn-as-static or mac-move still enabled.`

- A maximum of 64 MACs can be configured on a port. If total number of configured MACs are greater than 64, then, enabling **mac-move** displays an error message:
  `ERROR: Cannot enable mac-move as total count of the MACs(p-static/static) is greater than 64.`

- Consider that **admin-status** and operation status of a port is disabled using **port-security** command with **port-security chassis convert-to-static** option and **port-security shutdown no-aging** option enabled.
  Now, if user changes the **admin-status** from **disabled** to **locked**, CLI displays an error message:
  `ERROR: LPS admin status cannot be locked for LPS admin disabled port`
  as it is not a valid configuration.

- When **mac-move** is enabled while the default VLAN is moved, if any one of the static MACs are learned on any other port on the VLAN to be moved, the default VLAN change is allowed and one of the static MAC is marked as valid on current port and duplicate on another port.
  For example,
  - port 1/1 is on default VLAN 10 and it has learned static MAC 00:00:00:00:00:01
  - port 1/2 is on default VLAN 20 and it also learns same static MAC 00:00:00:00:00:01
  If default VLAN 10 on port 1/1 is changed to VLAN 20 then static MAC 00:00:00:00:00:01 on port 1/1 is marked with duplicate (STATIC(*)) and port 1/2 as valid (STATIC)

- When **mac-move** is enabled, pure static MACs are learned as static on new port and marked as duplicate MAC entries on old port. Thus duplicate MAC entries are stored on multiple ports.

- When **mac-move** is disabled then, a port specific entry with action is created in the system for all duplicate static MACs at that instance. When **mac-move** is disabled, the 64 MAC restriction does not apply.

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 2 no-aging enable mac-move enable
-> port-security shutdown 0 no-aging disable
-> port-security shutdown 0 no-aging enable
-> port-security shutdown 0 no-aging enable learn-as-static enable
-> port-security shutdown 0 convert-to-static enable no-aging enable
-> port-security shutdown 0 no-aging enable convert-to-static enable boot-up enable
```

Release History

Release 6.6.1; command introduced.
Release 6.6.3; **no-aging** and **boot-up** parameters added.
Release 6.6.4; **learn-as-static** and **mac-move** parameters added.

Related Commands

port-security	Enables or disables LPS on the switch ports.
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 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
   lpsConvertToStatic
   lpsLearningWindowBootupStatus
   lpsLearningWindowExpiryStatus
   lpsLearningWindowLearnAsStatic
   lpsLearningWindowPseudoMacMove
```

port-security maximum

Specifies the maximum number of source MAC addresses that an LPS port is allowed to learn.

port-security *slot/port***[**-*port2***]** **maximum** *num* **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).
maximum *num*	The number of source MAC addresses that are allowed on this port. Valid range is 1-1000.
learn-trap-threshold *num*	The number of bridged MAC address to learn before sending traps. Valid range is 0 to maximum number of MAC addresses configured on LPS port.

Defaults

By default, the number of MAC addresses allowed is set to 1.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If the port attempts to learn a MAC address that exceeds the maximum number allowed, the port blocks the unauthorized address, or shuts down the port. Use the **port-security violation** command to specify how an LPS port handles the violating traffic.
- 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.
- Reducing the **maximum** to a lower value than the number of static MACs learned on the port is not allowed. For example, consider a scenario where maximum MAC address set on a port is 5 and it learned 3 static Mac's. If Maximum is changing to less than 3, then the following error message is displayed:
  "`ERROR: Maximum MACs should be the same or greater than the static MAC configured on the port`"

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 6.6.1; command introduced.
Release 6.6.3; **learn-trap-threshold** parameter added.

Related Commands

port-security	Enables or disables LPS on the switch ports.
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).
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 6450, 6350

Usage Guidelines

- The MAC addresses entering the LPS enabled port is learned as filtered MAC.
- The maximum filtering value is separate from the maximum bridged MAC address value.
- 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.
- When the number of filtered MAC addresses learned on the port reaches the maximum configured value, either the port is disabled (shutdown violation mode) or the MAC address learning is disabled (restrict violation mode).

Examples

```
-> port-security 1/10 max-filtering 6
-> port-security 1/10-13 max-filtering 18
```

Release History

Release 6.6.1; command introduced.

Related Commands

port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port 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 6450, 6350

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 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 6.6.1; command introduced.

Related Commands

port-security	Enables or disables LPS on the switch ports.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port 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 6450, 6350

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 that 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 three configured authorized MAC addresses and the maximum number of addresses allowed is set to ten, then only seven additional MAC addresses are allowed on that port.
- A static MAC address cannot be configured on a mobile 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 6.6.1; command introduced.

Related Commands

port-security	Enables or disables LPS on the switch ports.
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 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 a 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***]**

no 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). A port can have up to eight MAC ranges configured.
-*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 MAC addresses (for example, 00:20:95:00:10:2A).
high *mac_address*	MAC address that defines the high end of a range of MAC addresses (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 6450, 6350

Usage Guidelines

- By default, each LPS port is set to a range of 00:00:00:00:00:00–ff:ff:ff:ff:ff:ff, which includes all MAC addresses.
- Source MAC addresses received on an LPS port that are within the authorized range is 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 ten, then only seven additional MAC addresses are allowed on that port.
- Multiple MAC range can be configured for a port. A maximum of eight MAC range can be configured per port.

- To modify the configured MAC range, the existing configuration must be deleted before adding the new configuration.
- A MAC range can be part of multiple ports but a single port cannot have duplicate MAC range.
- A MAC range cannot overlap with another MAC range configured for the port.
- To delete the configured MAC range, use the **no** form of the command.
- The default MAC range is automatically applied when all the configured MAC range for the port is deleted.

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

-> port-security 1/5 mac-range low 00:01:01:22:22:56 high 00:01:01:22:22:67
-> port-security 1/5 mac-range low 00:01:01:22:33:56 high 00:01:01:22:33:67
-> port-security 1/5 mac-range low 00:01:01:22:44:56 high 00:01:01:22:44:67
-> port-security 1/5 mac-range low 00:01:22:22:11:56 high 00:01:22:22:11:67
-> port-security 1/5 mac-range low 00:01:22:22:22:56 high 00:01:22:22:22:67
-> port-security 1/5 mac-range low 00:01:22:22:33:56 high 00:01:22:22:33:67
-> port-security 1/5 mac-range low 00:01:22:22:44:56 high 00:01:22:22:44:67
-> port-security 1/5 mac-range low 00:01:22:22:55:56 high 00:01:22:22:55:67

-> no port-security 1/5 mac-range low 00:01:01:22:33:56 high 00:01:01:22:33:67
```

Release History

Release 6.6.1; command introduced.
Release 6.7.2.R05; ability to configure multiple MAC range per port added.

Related Commands

port-security	Enables or disables LPS on the switch ports.
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 is allowed to learn.
port-security violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.
show port-security	Displays the LPS configuration and the table entries.

MIB Objects

```
learnedPortSecurityTable
   lpsLoMacRange
   lpsHiMacRange
```

```
   lpsRowStatus
learnedPortSecurityL2MacRangeTable
   lpsL2LowMacAddress
   lpsL2HighMacAddress
```

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	All the learned MAC addresses are flushed and no traffic is allowed on the port, but the port link status remain up.
shutdown	All the learned MAC addresses are flushed and no traffic is allowed on the port, and the port link is brought down.

Defaults

By default, the security violation mode is set to **restrict** when LPS is enabled on the port.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When a traffic violation occurs on an LPS port, notice is sent to the Switch Logging task.
- When a port is shut down 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.
- If the violation mode is set to **restrict**, unauthorized source MAC addresses are not learned in the LPS table but are recorded in the source learning MAC address table with a FILTER operational status. This allows the user to view MAC addresses that were attempting unauthorized access to the LPS port. The violating MAC is also shown in the **show port-security** command output.
- 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 6.6.1; command introduced.
Release 6.6.3; **discard** parameter added.

Related Commands

port-security	Enables or disables LPS on the switch ports.
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 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 an LPS violation. The specified port resumes normal operation without having to manually reset the port or the entire slot.

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 slot (for example, 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 6450, 6350

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 6.6.1; command introduced.

Related Commands

port-security	Enables or disables LPS on the switch ports.
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 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 6450, 6350

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 6.6.1; command introduced.

Related Commands

show port-security	Displays the LPS configuration and the table entries.

MIB Objects

```
learnedPortSecurityTable
   lpslearnedrapThreshold
```

show port-security

Displays the LPS configuration and the table entries. Also displays the multiple MAC address range configured for the port.

show port-security [*slot/port1-port2* | *slot/port***] [mac-range]**

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 must 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 6450, 6350

Usage Guidelines

- This command 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.
- MAC addresses learned on the LPS port 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 the 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.
- When **mac-move** is enabled using **port-security shutdown** command, pure static MACs are learned as static on new port and marked as duplicate MAC entries on old port. Thus duplicate MAC entries are stored on multiple ports and displayed with (*).
- To view the multiple MAC range configured for the port, use the parameter **mac-range** in the command. Specify the slot and port to view the MAC range configured for the specific port.

Examples

```
-> show port-security

Legend: Mac Address: * = Duplicate Static
        Mac Address: # = Pseudo Static
Port:  1/2
 Operation Mode   :                ENABLED,
 Max MAC bridged  :                      6,
 Trap Threshold   :               DISABLED,
 Max MAC filtered :                      5,
 Violation        :               RESTRICT,
 Violating MAC    :                   NULL

MAC Address        VLAN   TYPE
-------------------+------+--------+-----------
 00:00:00:00:00:01    1    STATIC
00:00:00:00:00:02     1    STATIC(*)
00:00:00:00:00:02     1    STATIC(#)
00:00:00:00:00:13     1    STATIC
 00:00:00:00:00:14    1    STATIC
 00:00:00:00:00:20    1    STATIC
```

Output for port violation in **restrict** mode.

```
-> show port-security

Legend: Mac Address: * = Duplicate Static
Mac Address: # = Pseudo Static

Port:  1/7
Operation Mode   :             RESTRICTED,
Max MAC bridged  :                      1,
Trap Threshold   :               DISABLED,
Max MAC filtered :                      5,
Violation        :               RESTRICT,
Violating MAC    :      00:00:00:00:00:08,

MAC Address        VLAN   TYPE
-------------------+------+------------
00:00:00:00:00:06    10   FILTER
00:00:00:00:00:07    10   FILTER
00:00:00:00:00:20    10   STATIC
00:00:00:00:00:21    10   FILTER
00:00:00:00:00:22    10   FILTER
00:00:00:00:00:23    10   FILTER

-> show port-security 1/5 mac-range
Port            Low MAC           High MAC
-----+-----------------+------------------
1/5   00:01:01:22:22:56 00:01:01:22:22:67
1/5   00:01:01:22:33:56 00:01:01:22:33:67
1/5   00:01:01:22:44:56 00:01:01:22:44:67
1/5   00:01:22:22:11:56 00:01:22:22:11:67
1/5   00:01:22:22:22:56 00:01:22:22:22:67
1/5   00:01:22:22:33:56 00:01:22:22:33:67
1/5   00:01:22:22:44:56 00:01:22:22:44:67
```

```
1/5   00:01:22:22:55:56 00:01:22:22:55:67

-> show port-security mac-range
Port            Low MAC           High MAC
-----+----------------+-----------------
1/5   00:01:01:22:22:56 00:01:01:22:22:67
1/5   00:01:01:22:33:56 00:01:01:22:33:67
1/5   00:01:01:22:44:56 00:01:01:22:44:67
1/5   00:01:22:22:11:56 00:01:22:22:11:67
1/5   00:01:22:22:22:56 00:01:22:22:22:67
1/5   00:01:22:22:33:56 00:01:22:22:33:67
1/5   00:01:22:22:44:56 00:01:22:22:44:67
1/5   00:01:22:22:55:56 00:01:22:22:55:67
1/3   00:00:00:00:00:38 00:00:00:00:00:40
1/3   00:00:00:00:00:41 00:00:00:00:00:44
1/3   00:00:00:00:00:45 00:00:00:00:00:48
1/3   00:00:00:00:00:49 00:00:00:00:00:52
```

output definitions

MAC Address	Duplicate Static: On an LPS port, static MAC can be configured on more than one port on a VLAN. The first configured entry, and the port where the MAC is ingressing is marked as VALID. Pseudo Static: The MAC addresses that are learned dynamically in the system and are converted to static in the hardware.
Port	The module slot number and the physical port number on that module.
Operation Mode	The LPS 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 MAC addresses 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 MAC Address that caused the violation on this port.
Violating MAC	An individual authorized MAC address. Configured through the **port-security mac** command.

output definitions

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 the configuration is saved and reboot of the switch. When MAC is already present on old port as permanent static, the entry is not deleted, but marked as duplicate **STATIC (*)** and MAC on the new port is learned as pseudo-static **STATIC (#)**. When port violation is set to restrict, then, **STATIC** and **FILTER** options are displayed**.**

Release History

Release 6.6.1; command introduced.
Release 6.6.3; **Legend** and **Violating MAC** fields added
Release 6.7.2.R05; **mac-range** parameter added.

Related Commands

show port-security shutdown	Displays the amount of time during which source learning can occur on all LPS ports.
port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on a port.

MIB Objects

```
learnedPortSecurityTable
   lpsMaxMacNum
   lpsMaxFilteredMacNum
   lpsLoMacRange
   lpsHiMacRange
   lpsViolationOption
   lpsMaxFilteredMacNum
   lpsViolatingMac
   lpsOperStatus
   lpsRelease
learnedPortSecurityL2MacRangeTable
   lpsL2LowMacAddress
   lpsL2HighMacAddress
```

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 6450, 6350

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       =  5,
Convert-to-static         =  DISABLE,
No Aging                  =  ENABLE,
Boot Up                   =  ENABLE,
Learn As Static           =  ENABLE,
Mac Move                  =  ENABLE,
Remaining Learning Window =  289 sec

-> show port-security shutdown
LPS Shutdown Config       =  Infinity,
Convert-to-static         =  DISABLE,
No Aging                  =  ENABLE,
Boot Up                   =  ENABLE,
Learn As Static           =  ENABLE,
Mac Move                  =  ENABLE,
Remaining Learning Window =  Infinite Window
```

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 dynamic MAC addresses are converted to static MAC addresses (**enabled** or **disabled**). When enabled, MAC-addresses learned during learning window are converted into static MAC addresses.
No Aging	Indicates whether learned MAC addresses can age out or get flushed during the LPS learning window time period (**disabled** or **enabled**). When enabled, MAC-addresses learned during learning window are retained and not flushed.
Boot Up	Indicates whether the learning window automatically starts when the switch boots up (**Enable** or **disabled**). When **Boot Up** is enabled, Learning window starts at boot-up time when the switch restarts.
Mac-move	Allows the movement of pseudo static/static MAC addresses when enabled.
Learn-as-static	When enabled, the MAC is learned as a static address during learning window.
Remaining Learning Window	The remaining amount of time during which the LPS port can learn MAC addresses.

Release History

Release 6.6.1; command introduced.
Release 6.6.3; **No Aging** and **Boot Up** fields added.
Release 6.6.4; **Mac-move** and **Learn-as-static** fields added**.**

Related Commands

port-security learn-trap-threshold	Configures the number of bridged MAC addresses to learn before sending a trap.

MIB Objects

```
learnedPortSecurityGlobalGroup
   lpsLearningWindowNoAging
   lpsLearningWindowBootupStatus
   lpsLearningWindowExpiryStatus
   lpsLearningWindowLearnAsStatic
   lpsLearningWindowPseudoMacMove
   lpsConvertToStatic
   lpsLearningWindowTime
   lpsLearningWindowTimeWithStaticConversion
```

show port-security brief

Displays per port LPS parameters configured for all the ports.

show port-security brief

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command displays the configured LPS parameters. The parameters are displayed even if the LPS is disabled on the port.
- The status of the LPS port is displayed according to the admin status set by **port-security admin status** command and the operational status set by the **port-security shutdown** command. The status can be:
  – Enabled
  – Restricted (admin status is enabled)
  – Shutdown (admin status is enabled)
  – Discard (admin status is enabled)
  – Disabled
  – Locked

Operational Mode/ Admin Status	Enabled	Discard	Restrict	Shutdown
Enabled	Enabled	Discard	Restrict	Shutdown
Disabled	Disabled	Disabled	Disabled	Disabled

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 (for example, 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 learned on corresponding port.
Nb Macs Filtered	Number of filtered MAC address learned on corresponding port.
Nb Macs Static	Number of static MAC address configured on corresponding port.

Release History

Release 6.6.3; command introduced.

Related Commands

port-security maximum	Configures the maximum number of source MAC addresses that an LPS port is allowed to learn.
port-security max-filtering	Configures the maximum number of MAC addresses that can be filtered on the LPS ports.

MIB Objects

```
learnedPortSecurityTable
   lpsMaxMacNum
   lpsMaxFilteredMacNum
   lpsMaxStaticMacNum
   lpsOperStatus
   lpsAdminStatus
   lpsViolatingMac
```

23 Ethernet Port Commands

The Ethernet port software is responsible for configuring and monitoring Ethernet ports. This software provides the following functionalities:

- 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 autoneg** **interfaces crossover** **interfaces pause** **interfaces duplex** **interfaces admin** **interfaces alias** **interfaces ifg** **interfaces no l2 statistics** **interfaces max frame** **interfaces flood enable** **interfaces flood rate** **interfaces clear-violation-all** **interfaces tdr-test-start** **interfaces no tdr-statistics** **interfaces tdr-extended-test-start** **interfaces no tdr-extended-statistics** **interfaces transceiver ddm** **interfaces eee** **show interfaces** **show interfaces tdr-statistics** **show interfaces tdr-extended-statistics** **show interfaces capability** **show interfaces flow control** **show interfaces pause** **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** **show interfaces eee**

Combo port commands	**interfaces clear-violation-all** **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 flow control** **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** **show interfaces hybrid ifg**
Interface violation commands	**interfaces violation-recovery-time** **interfaces violation-recovery-maximum** **interfaces violation-recovery-trap** **interfaces clear-violation-all** **show interfaces violation-recovery**
Link Fault Propagation group commands	**link-fault-propagation group** **link-fault-propagation group admin-status** **link-fault-propagation group source** **link-fault-propagation group destination** **link-fault-propagation group wait to shutdown** **show link-fault-propagation group**
IEEE 1588 Precision Time Protocol (PTP) commands	**interfaces ptp** **show interfaces ptp** **show interfaces ptp-statistics**

trap port link

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

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
enable	Port link up/down traps are displayed on the NMS.
disable	Port link up/down traps are not displayed on the NMS.
on	Same as **enable**.
off	Same as **disable**.

Defaults

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

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

show interfaces status	Displays interface line settings.

MIB Objects

```
esmConfigTable
   esmPortSlot
```

```
esmPortIF
```

interfaces speed

Configures interface line speed.

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
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 Mb.
10000	Sets the interface to 10 Gb.
max 100	Sets the maximum speed to 100 Mb.
max 1000	Sets the maximum speed to 1000 Mb (one Gigabit).

Defaults

parameter	default
auto | 10 | 100 | 1000 | 10000 | max 100 | max 1000}	Auto (copper ports); 1000 (fiber ports);

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- The **auto** option sets the speed to auto-sensing.
- Configuration changes made with the **interfaces speed** command on the combo ports configured as either forced fiber or preferred fiber is applicable only on the SFP fiber ports and not the copper RJ-45 ports. See the **interfaces hybrid speed** command for more information.
- Configuration changes made with the **interfaces speed** command on the combo ports configured as either forced copper or preferred copper is applicable only on the copper RJ-45 ports and not the SFP fiber ports. See the **interfaces hybrid speed** command for more information.

Examples

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

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

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces duplex	Configures duplex mode.
interfaces autoneg	Enables and disables autonegotiation.
show interfaces status	Displays interface line settings.

MIB Objects

```
esmConfTable
   esmPortCfgSpeed
```

interfaces autoneg

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

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
enable	Enables autonegotiation.
disable	Disables autonegotiation.
on	Same as enable.
off	Same as disable.

Defaults

parameter	default
enable | disable | on | off	enable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- If autonegotiation is disabled, auto MDIX, auto speed, and auto duplex are not accepted. See the **interfaces crossover** command on page 23-10 for more information.
- Configuration changes made with the **interfaces autoneg** command on the combo ports configured as either forced fiber or preferred fiber is applicable only on the SFP fiber ports and not the copper RJ-45 ports. See the **interfaces hybrid autoneg** command for more information.
- Configuration changes made with the **interfaces autoneg** command on combo ports configured as either forced copper or preferred copper is applicable only on the copper RJ-45 ports and not the SFP fiber ports. See the **interfaces hybrid autoneg** command for more information.
- Disabling autonegotiation is not supported on copper Gigabit ports.

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces speed	Configures interface speed.
interfaces crossover	Configures crossover port settings.
show interfaces status	Displays interface line settings.
show interfaces capability	Displays autonegotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgAutoNegotiation
```

interfaces crossover

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

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
auto	The interface automatically detects the 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

parameter	default
auto | mdix | mdi (all copper ports)	auto

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- If autonegotiation is disabled, then the automatic crossover is also disabled. See the **interfaces autoneg** command on page 23-8 for more information.
- You cannot configure crossover settings on fiber ports. These ports use the MDI standard.
- Configuration changes made with the **interfaces crossover** command on combo ports configured as either forced copper or preferred copper is applicable only on the copper RJ-45 ports and not the SFP fiber ports. See the **interfaces hybrid crossover** command for more information.

Examples

```
-> interfaces 3 crossover mdi
-> interfaces 3/1 crossover mdix
-> interfaces 3/1-4 crossover auto
```

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces speed	Configures interface speed.
interfaces autoneg	Enables and disables autonegotiation.
show interfaces status	Displays interface line settings.
show interfaces capability	Displays autonegotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
   esmPortCfgCrossover
```

interfaces pause

Configures whether the switch honors or transmits and honors the flow control PAUSE frames on the specified interface. PAUSE frames are used to pause the flow of traffic between two connected devices to help prevent packet loss when traffic congestion occurs between switches.

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
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 6450, 6350

Defaults

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

Usage Guidelines

- Flow control is only supported on a standalone switch. It is not supported in a stackable configuration.
- 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. The operational settings as shown in the following table, override the configured settings as long as both autonegotiation and flow control are 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.

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

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

MIB Objects

```
esmConfigTable
   esmPortCfgFlow
dot3PauseTable
   dot3PauseAdminMode
```

interfaces duplex

Configures duplex mode. In full duplex mode, the interface transmits and receives data simultaneously. In half duplex mode, the interface can transmit *or* receive data at a given time. Auto duplex setting causes the switch to advertise all available duplex modes (half/full/both) for the port during autonegotiation.

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
full	Sets interface to full duplex mode.
half	Sets interface to half duplex mode.
auto	Switch automatically sets both the duplex mode settings to autonegotiation.

Defaults

parameter	default
full | half | auto	**full**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- If a port is detected as Gigabit (1000 Mbps), half duplex mode is not supported on the Gigabit modules.
- Configuration changes done with the **interfaces duplex** command on the combo ports configured as either forced copper or preferred copper is applicable only on the copper RJ-45 ports and not the SFP fiber ports. See the **interfaces hybrid duplex** command for more information.

Examples

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

Release History

Release 6.6.1; command 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* **[**/*port***[**-*port2***]] admin {up | down}**

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
up	Enables the interface.
down	Disables the interface.

Defaults

parameter	default
up | **down**	up

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces tdr-test-start	Displays general interface information (for example, hardware, MAC address, input errors, and output errors).
show interfaces port	Displays port status (up or down).

MIB Objects

```
ifTable
   ifAdminStatus
```

interfaces alias

Configures a description (alias) for a single port.

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
description	A description for the port, which can be up to 64 characters long. Spaces must be contained within quotes (for example, “IP Phone”).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You can only configure one port at time. You cannot configure an alias for multiple ports.
- 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 SFP port and to the copper RJ-45 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 6.6.1; command introduced.

Related Commands

interfaces tdr-test-start	Displays general interface information (for example, hardware, MAC address, input errors, and output errors).
show interfaces port	Displays port status (up or down) and any aliases for a port.

MIB Objects

```
ifXTable
   ifAlias
```

interfaces ifg

Configures the inter-frame gap on Gigabit Ethernet interfaces.

interfaces *slot* **[**/*port***[**-*port2***]] ifg** *bytes*

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
bytes	Inter-frame gap value, in bytes. Valid range is 9–12.

Defaults

parameter	default
bytes	12

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

You can only configure one slot at a time. Repeat the command to configure additional slots.

Examples

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

Release History

Release 6.6.1; command 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.

[stacking] interfaces *slot* **[**/*port***[**-*port2***]] no l2 statistics**

Syntax Definitions

stacking	Clears the counter statistics for the specified stack port.
slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- This command calls for an upper or lower case “L” character in front of the “2” character. Entering the digit “1” (one) results in an error message.
- The “**stacking**” parameter is not supported in OmniSwitch 6350, since it is a stand alone model.

Examples

```
-> interfaces 3/1 no l2 statistics
-> interfaces 3 no l2 statistics
-> interfaces 3/1-6 no l2 statistics
-> stacking interfaces 3/52 no l2 statistics
```

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces tdr-test-start	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
   esmStackPortClearStats
```

interfaces max frame

Configures the maximum frame size for Gigabit Ethernet interfaces.

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
max frame	Maximum frame size, in bytes. Valid range is 1518–9216.

Defaults

parameter	default
bytes (Gigabit Ethernet Packets)	9216
bytes (Ethernet Packets)	1553

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces tdr-test-start	Displays general interface information (for example, hardware, MAC address, input errors, and output errors).

MIB Objects

```
esmConfTable
   esmPortCfgMaxFrameSize
```

interfaces flood enable

Enables flood rate limiting based on a storm type on the specified interface.

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

Syntax Definitions

slot	Slot you want to configure (for example, 3).
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
all	Enables for all types of storms.
enable	Enables storm control.
disable	Disables storm control.

Defaults

parameter	default
broadcast	**enable**
unknown-unicast	**enable**
multicast	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- Applying the peak flood rate value to multicast traffic also limits IP Multicast Switching (IPMS) and non-IPMS multicast traffic.
- The peak flood rate value is configurable through the **interfaces flood rate** command.
- When multicast rate limiting is disabled, the peak flood rate value for the interface is no longer applied to multicast traffic. This change does not prevent the normal flow of multicast traffic on the specified interface.

Examples

```
-> interfaces 4/1 flood unknown-unicast enable
-> interfaces 4/1 flood unknown-unicast disable
-> interfaces 4 flood all enable
```

Release History

Release 6.6.4; command introduced.

Related Commands

show interfaces flood rate	Displays interface peak flood rate settings.
interfaces flood rate	Configures the rate limit based on storm type. The measurement unit for rate limit is Mbps, PPS and percentage.

MIB Objects

```
esmConfTable
   esmPortFloodMcastEnable
   esmPortFloodBcastEnable
   esmPortFloodUnknownUcastEnable
```

interfaces flood rate

Configures the rate limit based on storm type. The measurement unit for rate limit is Mbps, PPS and percentage.

interfaces *slot* **[**/*port***[**-*port2***]] flood {broadcast | multicast | unknownunicast | all} rate {mbps** *num* **| pps** *num* **| percentage** *num* **| default}**

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
rate	Configures the rate limiting and high threshold value.
default	Configures default rate limit value.
all	Configures for all types of storm.
num	Specify flood rate, in megabits per second (Mbps).
pps	Packets per second.

Defaults

parameter	default
Mbps (10 Ethernet)	4
Mbps (100 Fast Ethernet)	49
Mbps (Gigabit Ethernet)	496
Mbps (10 Gigabit Ethernet)	997

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If rate is configured in Mbps, then minimum value that can be configured is 1 and maximum is up to port bandwidth.
- In case of PPS, final rate will be calculated based on packet size of 512 bytes. For example, 244 is the minimum value that can be configured as it is equivalent to 1 Mbps (244*512*8 bits) and the maximum number for PPS can be configured is based on port current bandwidth.
- Rate limit value will be changed, if configured rate limit is greater than the detected port speed bandwidth. For example, if port speed bandwidth is 1000 Mbps and rate is configured for any storm type is 200 Mbps. If port comes up with 100 Mbps speed, then the rate limiting will converted to default value (49 Mbps) for 100 Mbps.
- The auto recovery is not enabled by default.

- If the port range contains invalid ports, no configuration will be applied for any of the port given in that range.

Examples

```
-> interfaces 4/1 flood unknown-unicast rate mbps 50
-> interfaces 4 flood broadcast rate pps 500
-> interfaces 4/1-2 flood multicast rate default
-> interfaces 4/1 flood all rate default
```

Release History

Release 6.6.4; command introduced.

Related Commands

show interfaces flood rate	Displays interface peak flood rate settings.
interfaces flood enable	Enables/disables flood rate limiting for multicast traffic on an interface.

MIB Objects

```
esmConfTable
   esmPortMaxFloodRate
   esmPortMaxUnknownUcastFloodRate
   esmPortMaxMcastFloodRate
   esmPortMaxFloodRateLimit
   esmPortMaxUnknownUcastFloodRateLimit
   esmPortMaxMcastFloodRateLimit
```

interfaces clear-violation-all

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

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

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

Release History

Release 6.6.1; command introduced.

Related Commands

show interfaces port	Displays interface port status.

MIB Objects

```
esmConfTable
   esmPortViolationClearAll
```

interfaces hybrid autoneg

Enables or disables autonegotiation on a single combo port, a range of combo ports, or all combo ports on a switch.

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
fiber	Specifies that configuration changes are made to the SFP ports.
copper	Specifies that changes are made to the copper RJ-45 ports.
enable	Enables autonegotiation.
disable	Disables autonegotiation.
on	Same as enable.
off	Same as disable.

Defaults

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

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The MIB table and MIB object listed in the following “MIB Objects” section 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.

Examples

```
-> interfaces 1/25 hybrid copper autoneg disable
-> interfaces 1/25-26 hybrid copper autoneg disable
-> interfaces 1 hybrid copper autoneg disable
```

Release History

Release 6.6.1; command 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 autonegotiation, 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* **[**/*port***[**-*port2***]] hybrid copper crossover {auto | mdix | mdi}**

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
copper	Specifies that changes are made to the copper RJ-45 ports.
auto	The interface automatically detects the 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

parameter	default
auto | mdix | mdi	**auto**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- You cannot configure crossover settings on fiber ports. These ports use the MDI standard.
- The MIB table and MIB object listed in the following “MIB Objects” section apply to the inactive configured media only. See the “MIB Objects” section in the **interfaces crossover** section for the MIB table and MIB object for the active configured media.

Examples

```
-> interfaces 1/25 hybrid copper crossover disable
-> interfaces 1/25-26 hybrid copper crossover mdix
-> interfaces hybrid copper crossover auto
```

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces hybrid speed	Configures interface speed for combo ports.
interfaces hybrid autoneg	Enables and disables autonegotiation 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 autonegotiation, 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***[**/*port***[**-*port2***]] hybrid {fiber | copper} duplex {full | half | auto}**

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
fiber	Specifies that configuration changes are made to the SFP ports.
copper	Specifies that changes are made to the copper RJ-45 ports.
full	Sets interface to full duplex mode.
half	Sets interface to half duplex mode.
auto	Switch automatically sets both the duplex mode settings to autonegotiation.

Defaults

parameter	default
full | half | auto	**auto**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The MIB table and MIB object listed in the following “MIB Objects” section 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.

Examples

```
-> interfaces 1/25 hybrid copper duplex auto
-> interfaces 1/25-26 hybrid copper duplex half
-> interfaces 1 hybrid copper fiber full
```

Release History

Release 6.6.1; command 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***[**/*port***[**-*port2***]] speed hybrid {fiber | copper} {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}**

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
fiber	Specifies that configuration changes are made to the SFP ports.
copper	Specifies that changes are made to the copper RJ-45 ports.
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 one Gigabit.
10000	Sets the interface to ten Gigabit. This option is currently not supported.
max 100	Sets the maximum speed to 100 Mb.
max 1000	Sets the maximum speed to 1000 Mb (one Gigabit).

Defaults

parameter	default
auto | 10 | 100 | 1000 | 10000 | max 100 | max 1000	**auto**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The MIB table and MIB object listed in the following “MIB Objects” section 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.

Examples

```
-> interfaces 1/25 hybrid copper speed auto
-> interfaces 1/25-26 hybrid copper speed 100
-> interfaces 1/25 hybrid fiber speed 1000
```

Release History

Release 6.6.1; command introduced.

Related Commands

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

MIB Objects

```
esmHybridConfTable
   esmHybridPortCfgSpeed
```

interfaces hybrid pause

Configures whether the switch honors or transmits and honors the flow control PAUSE frames on the specified combo port. PAUSE frames are used to pause the flow of traffic between two connected devices to help prevent packet loss when traffic congestion occurs between switches.

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

Syntax Definitions

slot	Slot number you want to configure.
port	Port number of the interface you want to configure.
port2	Last port number in a range of ports you want to configure.
fiber	Specifies that configuration changes are made to the SFP ports.
copper	Specifies that changes are made to the copper RJ-45 ports.
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 6450, 6350

Defaults

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

Usage Guidelines

- 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. The operational settings as shown in the following table, override the configured settings as long as both autonegotiation and flow control are 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

Configured Local Tx	Configured Local Rx	Configured Remote Tx	Configured Remote Rx	Negotiated Local Tx	Negotiated Local Rx
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.

Examples

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

Release History

Release 6.6.1; command 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
```

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 traveled in the 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	Slot number of the module.
port	Physical Port of the module.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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, combo ports or stacking ports.
- TDR test is not supported on 10 Mbps speed.
- No range support is provided in the configuration CLI as only one test can be started at a time.
- Last TDR results for a port will automatically get cleared on start of every new TDR test.
- TDR test takes approximately 12-15 seconds for execution, It is preferable to try the test multiple times till a result of either pass or fail is received.

Examples

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

Release History

Release 6.6.4; command 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 test performed on the port.

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

Syntax Definitions

slot	Slot number of the module.
port	Physical port of the module. For example, 3/1 specifies port 1 on slot 3.
port2	Physical port range of the module. For example, 3/1-7 specifies slot/port 1 - port2.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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. This is in synchronization with existing interface commands. Highest level granularity supported for clear statistics is per slot.

Examples

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

Release History

Release 6.6.4; command 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
```

interfaces tdr-extended-test-start

Starts the extended cable diagnostics on a port.

interfaces [*slot* | *slot*/*port*] **tdr-extended-test-start**

Syntax Definitions

slot	Slot number of the module.
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 6450

Usage Guidelines

- No range support is provided in the configuration CLI as only one test can be started at a time.
- Last extended TDR results for a port will automatically get cleared on start of every new extended TDR test.
- Extended TDR operations cannot be performed on fiber/stacking ports.
- After changing the port speed, pair swap output shows crossover for straight cable and vice-versa, due to the crossover functionality available in hardware to automatically correct errors in cable selection. The device makes the necessary adjustment prior to commencing auto-negotiation. If the device interoperates with a device that implements MDI/MDIX crossover, a random algorithm is used to decide whether local/remote end will perform the crossover.
- Extended TDR test is not supported on combo ports.

Examples

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

Release History

Release 6.6.4; command introduced.

Related Commands

show interfaces tdr-extended-statistics	Displays the results of the last Extended TDR test performed on a port.
interfaces no tdr-extended-statistics	Used to clear the statistics of the last test performed on the port.

MIB Objects

```
esmTdrPortTable
   esmTdrPortTest
```

interfaces no tdr-extended-statistics

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

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

Syntax Definitions

slot	Slot number of the module.
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.
slot/*port***[**-*port2***]**	Physical port of the module. For example, 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 6450

Usage Guidelines

There is no global statistics clear command. This is in synchronization with existing interface commands. Highest level granularity supported for clear statistics is per slot.

Examples

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

Release History

Release 6.6.4; command introduced.

Related Commands

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

MIB Objects

```
esmTdrPortTable
   esmTdrPortClearResults
```

interfaces transceiver ddm

Enable or disable the DDM functionality globally.

interfaces transceiver ddm [trap] {enable | disable}

Syntax Definitions

enable	Enables DDM functionality.
disable	Disables DDM functionality.
trap	Enable or disable the DDM trap globally for DDM warning/alarm threshold violations.

Defaults

parameter	default
ddm	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- DDM capability will vary based on the transceiver manufacturer.
- Information will be read sequentially from a different SFP at predefined polling intervals. The number of SFPs in the switch will determine how often each SFP is polled and could result in longer delayed read times of over a minute.
- DDM trap can enabled only when DDM is enabled.

Examples

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

Release History

Release 6.6.4; command was introduced.
Release 6.7.2.R02; **trap** keyword added.

Related Commands

show interfaces transceiver	Displays the DDM information of the specified transceiver.

MIB Objects

```
ddmConfiguration
   ddmConfig
```

`ddmTrapConfig`

interfaces eee

Enables or disabled Energy Efficient Ethernet.

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

Syntax Definitions

slot	Slot to be configured (for example, 3).
port	Port number of the interface to be configured.
port2	Last port number in a range of ports to be configured.
enable	Enables EEE functionality.
disable	Disables EEE functionality.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- EEE is not supported on fiber ports or copper ports operating at 10Mbps speed.
- For copper ports operating at 10M speed EEE configuration is allowed but will have no affect. If the port speed is later changed to 100/1000M then EEE functionality is enabled.
- Enabling EEE will start advertising EEE capability to peers ports. Disabling EEE will stop advertising EEE capability to peer ports.

Examples

```
-> interfaces 1/1 eee enable
-> interfaces 2 eee disable
```

Release History

Release 6.6.4; command was introduced.

Related Commands

show interfaces eee	Displays the EEE information for the specified interface.

MIB Objects

```
esmConfTable
   esmPortCfgEeeStatus
```

interfaces ptp

Enables or disables IEEE 1588 Precision Time Protocol (PTP) on the switch.

interfaces ptp {enable | disable}

Syntax Definitions

enable	Enables IEEE 1588 Precision Time Protocol (PTP) functionality.
disable	Disables IEEE 1588 Precision Time Protocol (PTP) functionality.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450 (OS6450-P10S and OS6450-U24S only)

Usage Guidelines

- After entering **interfaces ptp enable**, the switch must be rebooted for the changes to take effect.
- When PTP is enabled, switches operate as standalone units and cannot become part of a stack (applies to OS6450-U24S models only).
- For OS6450-U24S switches to become part of a stack, PTP must be disabled. (After entering **interfaces ptp disable**, the switch must be rebooted for the changes to take effect.)
- In order for PTP to remain enabled following subsequent reboots of the switch, **interfaces ptp enable** must be written to the **boot.cfg** file using the **write memory** command.
- If an OS6450-XNI-U2 expansion module is installed in an OS6450-U24S on boot up, the switch will assume that it is a part of a stack, regardless of whether **interfaces ptp enable** has been written to the **boot.cfg** file. To enable PTP, the expansion module must be removed from the chassis and the switch must be rebooted with PTP enabled.

Examples

```
-> interfaces ptp enable
-> interfaces ptp disable
```

Release History

Release 6.6.5; command was introduced.

Related Commands

show interfaces ptp	Displays the current IEEE 1588 Precision Time Protocol (PTP) status on the switch.
show interfaces ptp-statistics	Displays IEEE 1588 Precision Time Protocol (PTP) ingress and egress statistics for each port.

MIB Objects

```
ptpConfiguration
```

show interfaces

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

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

Syntax Definitions

stacking	Displays information for stacking ports.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number (for example, 3).
- The operational status field in the show command indicates the interface status (up/down). The operational status of the port may be down due to admin action and software reasons such as violations caused due to STP, LPS-S, QOS, UDLD, NETSEC, NISUP, LLDP, RFP, LinkMon, LFP, LPS-D, STROM, LBD, STP-S, Admin-Down activity. Whenever the port is down, the "show interfaces" output displays the violation reason due to which the operational status of the port is down.
  - For example, if the violation is caused due to Learned Port Security, the operational status is displayed as ‘down, LPS’. If the violation caused is due to Spanning Tree Protocol, operational status is displayed as ‘down, STP’.
  - If the port is down due to any physical fault or ENI failure, 'none' will be displayed in the operational field.
  - If the port is down due to admin action, 'Admin-Down' will be displayed in the operational field.

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

-> show interfaces 1/1
Slot/Port  1/1  :
  Operational Status     : down, "LPS-S"
  Last Time Link Changed : TUE NOV 27 12:00:35 ,
  Number of Status Change: 1,
  Type                   : Ethernet,
  SFP/SFP+/XFP           :  10/100/1000 BaseX,
  MAC address            : e8:e7:32:e3:61:62,
  BandWidth (Megabits)   :     -   ,            Duplex           : -,
  Autonegotiation        :   1  [ 1000-F 100-F 100-H 10-F 10-H ],
  Long Frame Size(Bytes) : 9216,
  Rx             :
  Bytes Received  :             66879788, Unicast Frames :              130593,
  Broadcast Frames:                    0, M-cast Frames  :                  54,
  UnderSize Frames:                    0, OverSize Frames:                   0,
  Lost Frames     :                    0, Error Frames   :                   0,
  CRC Error Frames:                    0, Alignments Err :                   0,
  Tx             :
  Bytes Xmitted   :             67252462, Unicast Frames :              131354,
  Broadcast Frames:                    0, M-cast Frames  :                  34,
  UnderSize Frames:                    0, OverSize Frames:                   0,
  Lost Frames     :                    0, Collided Frames:                   0,
  Error Frames    :                    0

-> show stacking interfaces
 Slot/Port  1/51 :
  Operational Status     : down,
  Last Time Link Changed : FRI MAY 22 19:47:09 ,
  Number of Status Change: 0,
  Type                   : Stacking,
  BandWidth (Megabits)   :     -   ,            Duplex           : -,
  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
Slot/Port  1/52 :
 Operational Status     : up,
 Last Time Link Changed : FRI MAY 22 19:47:09 ,
 Number of Status Change: 1,
 Type                   : Stacking,
 BandWidth (Megabits)   :    10000,            Duplex           : Full,
 Rx              :
 Bytes Received  :           103100016, Unicast Frames :                85856,
 Broadcast Frames:                    0, M-cast Frames  :                   12,
 UnderSize Frames:                    0, OverSize Frames:                    0,
 Lost Frames     :                    0, Error Frames   :                    0,
 CRC Error Frames:                    0, Alignments Err :                    0,
 Tx              :
 Bytes Xmitted   :              3883702, Unicast Frames :                45872,
 Broadcast Frames:                 1948, M-cast Frames  :                  813,
 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).
Type	Interface type (Ethernet/Fast Ethernet/Gigabit Ethernet/stacking).
MAC address	Interface MAC address.
Bandwidth	Bandwidth (in megabits).
Duplex	Duplex mode (Half/Full/Auto).
Autonegotiation	The autonegotiation settings for this interface.
Long Accept	Long Frames status (enable/disable).
Runt Accept	Runt Frames status (enable/disable).
Long Frame Size	Long Frame Size (in Bytes).
Runt Size	Runt Frame Size (in Bytes).
Bytes Received	Number of Bytes received.
Rx Unicast Frames	Number of unicast frames received.
Rx Broadcast Frames	Number of broadcast frames received.
Rx M-cast Frames	Number of multicast frames received.
Rx Undersize Frames	Number of undersized frames received.
Rx Oversize Frames	Number of oversized frames received.
Rx Lost Frames	Number of Lost Frames received.

output definitions (continued)

Rx Error Frames	Number of error frames received.
Rx CRC Error Frames	Number of CRC error frames received.
Rx Alignments Err	Number of alignments error frames received.
Bytes Xmitted	Number of bytes transmitted.
Tx Unicast Frames	Number of unicast frames transmitted.
Tx Broadcast Frames	Number of broadcast frames transmitted.
Tx M-cast Frames	Number of multicast frames 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 6.6.1; command introduced.

Related Commands

show interfaces accounting	Displays interface accounting information (for example, packets received or 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
esmStackPortConfEntry
   esmStackPortSlotNum
   esmStackPortInOctets
   esmStackPortOutOctets
    esmStackPortInUcastPkts
    esmStackPortOutUcastPkts
    esmStackPortInMulticastPkts
    esmStackPortOutMulticastPkts
    esmStackPortInBroadcastPkts
    esmStackPortOutBroadcastPkts
    esmStackPortInPauseFrames
    esmStackPortOutPauseFrames
    esmStackPortStatsAlignmentErrors
    esmStackPortStatsFCSErrors
    esmStackPortInErrors
    esmStackPortOutErrors
    esmStackPortInDiscards
    esmStackPortOutDiscards
    esmStackPortTxCollisions
    esmStackPortRxUndersizePkts
    esmStackPortTxUndersizePkts
    esmStackPortRxOversizePkts
    esmStackPortTxOversizePkts
    esmStackPortAutoSpeed
```

show interfaces tdr-statistics

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

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

Syntax Definitions

slot	Slot number of the module.
slot/*port***[-***port2***]**	Physical port of the module. For example, 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 6450

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 Length accuracy may vary +/-2 meter
         Pair 1 - Orange and White
         Pair 2 - Green and White
         Pair 3 - Blue and White
         Pair 4 - Brown and White
 Slot/      Pair1       Pair1       Pair2       Pair2        Pair3      Pair3
Pair4        Pair4  Result
 Port        State        Length       State        Length        State
Length       State        Length
------+-----------------+------+-----------------+------+-----------------+-----
  1/5   open              32     open              33            open         33
  1/6   open              33    success             3            ok           3
```

```
-> show interfaces 1/1-2 tdr-statistics
Legend: Pair Length accuracy may vary +/-2 meter
        Pair 1 - Orange and White
        Pair 2 - Green and White
        Pair 3 - Blue and White
        Pair 4 - Brown and White
 Slot/      Pair1       Pair1       Pair2       Pair2        Pair3      Pair3
Pair4        Pair4  Result
 Port        State        Length       State        Length        State
Length       State        Length
------+-----------------+------+-----------------+------+-----------------+-----
  1/1   open              2      ok                0      ok                0
impedanceMismatch  4      success
  1/2   unknown           0      unknown           0      unknown           0
unknown            0      unknown
  1/3   unknown           0      unknown           0      unknown           0
unknown            0      unknown
  1/4   unknown           0      unknown           0      unknown           0
unknown            0      unknown
  1/5   open              32     open              33     open              33
open               33     success

-> show interfaces 1 tdr-statistics
Legend: Pair Length accuracy may vary +/-2 meter
        Pair 1 - Orange and White
        Pair 2 - Green and White
        Pair 3 - Blue and White
        Pair 4 - Brown and white
Slot/   No of     Cable         Pair1     Pair1     Pair2     Pair2     Pair3
Pair3     Pair4     Pair4     Test
port    pairs     State    Length    State     Length    State     Length    State
Length    State     Length   Result
------+-------+----------+--------+----------+--------+----------+--------+--------
1/1       4         ok    0          ok    3              ok    3             ok
3             ok   3      success
1/2       4    open-short    0     open-short    3      open-short    3     open-
short     3     open-short   3      success
1/3       4          open    0          open    3            open    3
open      3           open   3      success
1/4       4    Impedance-Mismatch    0     Impedance-Mismatch    3      Impedance-
Mismatch  3     Impedance-Mismatch    3     Impedance-Mismatch   3      success
1/5      4         short    0          short    3           short    3
short    3          short   3      success
1/6      4       unknown    0        unknown    0         unknown    0
unknown  0        unknown   0        fail
  .
  .
  .
  .
1/47  unknown           0      unknown           0      unknown           0
unknown            0      unknown
  1/48  unknown           0      unknown           0      unknown           0
unknown            0      unknown
  1/49  unknown           0      unknown           0      unknown           0
unknown            0      unknown
  1/50  unknown           0      unknown           0      unknown           0
unknown            0      unknown
```

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.
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) **Impedance Mismatch** - • Two cable of different quality/resistance are connected to each other through patch connector. • If the pair is short in a cable, it may affect the resistance of another pair hence it will result Impedance mismatch on that particular pair. (e) **Unknown** - Cable diagnostic test unable to find the state of a cable. (f) **Pair Swap** - Determines the channel associated with the MDI pair (cross or not for each two MDI pairs). (g) **Pair Polarity**- Detects if the pairs are connected with reverse polarity (reverse on one side between two conductors in one pair). (h) **Pair Skew**-The skew among the four pairs of cable (delay between pairs, in n-seconds). (i) **Cable Length** - The length of the cable, in meters. (j) **Downshift** - Gives the downshift status of the port, when the Gigabit link cannot be established.
Pair1 State	The state of the Pair 1 cable wire (**OK**, **Open**, **Short**, **Impedance Mismatch and 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**, **Impedance Mismatch and 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**, **Impedance Mismatch and 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, Impedance Mismatch and 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 6.6.4; command 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
   esmTdrPortPair1State,
   esmTdrPortPair1Length,
   esmTdrPortPair2State,
   esmTdrPortPair2Length,
   esmTdrPortPair3State,
   esmTdrPortPair3Length,
   esmTdrPortPair4State,
   esmTdrPortPair4Length,
   esmTdrResult
```

show interfaces tdr-extended-statistics

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

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

Syntax Definitions

slot	Slot number of the module.
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.
slot/*port***[**-*port2***]**	Physical port of the module. For example, 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 6450

Usage Guidelines

N/A

Examples

```
--> show interfaces 1/5 tdr-extended-statistics
Pair Swap
  Channel 1:straight
  Channel 2:straight
Pair Polarity
  Pair 1:positive
  Pair 2:positive
  Pair 3:positive
  Pair 4:positive
Pair Skew (in n-seconds)
  Pair 1:0
  Pair 2:0
  Pair 3:8
  Pair 4:0
Accurate Cable Length (in meters)
  Pair 1:15
  Pair 2:15
  Pair 3:15
  Pair 4:15
Downshift:No Downshift
```

output definitions

Pair Swap	Displays the channel associated with the MDI pair.
Pair Polarity	Displays if the pairs are connected with reverse polarity.
Pair Skew	Displays the skew among the four pairs of cable (delay between pairs, in n-seconds).
Accurate Cable Length	Displays the length of the cable, in meters.
Downshift	Displays the downshift status of the port, when the Gigabit link cannot be established.

Release History

Release 6.6.4; command introduced.

Related Commands

interfaces tdr-extended-test-start	Used to start the extended cable diagnostics on a port.
interfaces no tdr-extended-statistics	Used to clear the statistics of the last test performed on the port.

MIB Objects

```
esmTdrPortTable
   esmTdrPortPair1State,
   esmTdrPortPair1Length,
   esmTdrPortPair2State,
   esmTdrPortPair2Length,
   esmTdrPortPair3State,
   esmTdrPortPair3Length,
   esmTdrPortPair4State,
   esmTdrPortPair4Length,
   esmTdrResult
   esmTdrPortExtSwapTypePair1,
   esmTdrPortExtSwapTypePair2,
   esmTdrPortExtPolaritySwapPair1,
   esmTdrPortExtPolaritySwapPair2,
   esmTdrPortExtPolaritySwapPair3,
   esmTdrPortExtPolaritySwapPair4,
   esmTdrPortExtSkewPair1,
   esmTdrPortExtSkewPair2,
   esmTdrPortExtSkewPair3,
   esmTdrPortExtSkewPair4,
   esmTdrPortExtAccurateCableLenPair1,
   esmTdrPortExtAccurateCableLenPair2,
   esmTdrPortExtAccurateCableLenPair3,
   esmTdrPortExtAccurateCableLenPair4,
   esmTdrPortExtDownshiftStatus
```

show interfaces capability

Displays default autonegotiation, 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***[/***port***[-***port2***]]] capability**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The **show interfaces capability** command displays defaults settings in two rows of data for each port. The first row of data, identified by the label **CAP**, displays the valid user-defined configuration settings available for the port. The second row, identified by the label **DEF**, displays the default settings for the port.

Examples

```
-> show interfaces 5/1 capability
Slot/Port   AutoNeg     Flow   Crossover      Speed    Duplex
----------+---------+--------+-----------+----------+----------
  5/1  CAP     EN/DIS   EN/DIS  MDI/X/Auto  10/100/1G Full/Half
  5/1  DEF         EN       EN        Auto       Auto     Auto
```

output definitions

Slot	The slot number.
Port	The port number
AutoNeg	In the row labeled **CAP,** the field displays the valid autonegotiation configurations for the port. In the row label **DEF,** the field displays the default autonegotiation settings for the port. The possible values are **EN** (enabled) or **DIS** (disabled).
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).

output definitions (continued)

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**, **1 G**, **10/100/1 G**, **10 G**, 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 6.6.1; command introduced.

Related Commands

interfaces autoneg	Enables and disables autonegotiation.
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***[/***port***[-***port2***]]] flow [control]**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
control	Optional command syntax. It displays the same information as **show interfaces flow**.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, flow control wait time settings for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number, a range of ports by entering a slot and a range of ports. You can also display all interfaces in a slot by entering the slot number, or display all 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 6.6.1; command introduced.

Related Commands

interfaces crossover	Configures crossover settings.
show interfaces hybrid flow control	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 switch interfaces.

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

If a specific slot or slot/port number is not entered with this command, the flow control pause configuration for all switch interfaces is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Enter a slot and port number (for example, 3/21) or a range of port numbers (for example, 3/21-24) to display information for a specific port or a range of ports.
- Enter a slot number (for example, 1) to display information for all ports on a specific slot.

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 waits 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**). Configured through the **interfaces crossover** command.
Hybrid Type	The configured active media type for a hybrid port (**F** = fiber, **C** = copper, **NA** = not applicable).

Release History

Release 6.6.1; command 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 accounting

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

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, accounting information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number (for example, 3).
- For combo ports configured as either forced fiber or preferred fiber, the accounting information for the SFP fiber ports and not the copper RJ-45 ports is displayed. See the **show interfaces hybrid accounting** command for more information.
- For combo ports configured as either forced copper or preferred copper, the accounting information for the copper RJ-45 ports and not the SFP fiber port is displayed. See the **show interfaces hybrid accounting** command for more information.

Examples

```
-> show interfaces 1/2 accounting
1/2 ,
     Rx undersize packets         =                    0,
     Tx undersize packets         =                    0,
     Rx oversize packets          =                    0,
     Tx oversize packets          =                    0,
     Rx packets 64 Octets         =              3073753,
     Rx packets 65To127 Octets    =               678698,
     Rx packets 128To255 Octets   =                21616,
     Rx packets 256To511 Octets   =                21062,
     Rx packets 512To1023 Octets  =                    2,
     Rx packets 1024To1518 Octets =                   84,
     Rx packets 1519to4095 Octets =                    0,
     Rx packets 4096ToMax Octets  =                    0,
     Rx Jabber frames             =                    0
```

output definitions

Rx undersize packets	Number of undersized packets received.
Tx undersize packets	Number of undersized packets transmitted.
Rx oversize packets	Number of oversized packets received.
Tx oversize packets	Number of oversized packets transmitted.
Rx packets Octets	Number of packets received in each listed octet range.
Rx Jabber frames	Number of jabber packets received (longer than 1518 octets).
Tx deferred frames	Number of packets for which transmission was delayed (Ethernet only).

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces tdr-test-start	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 or transmitted).

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

Syntax Definitions

stacking	Displays information for stacking ports.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, counter information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number (for example, 3).
- These counters do not apply to Gigabit Ethernet traffic.
- For combo ports configured as either forced fiber or preferred fiber, statistics for the SFP fiber ports and not the copper RJ-45 ports is displayed. See the **show interfaces hybrid counters** command for more information.
- For combo ports configured as either forced copper or preferred copper, statistics for the copper RJ-45 ports and not the SFP fiber port is displayed. See the **show interfaces hybrid counters** command for more information.
- This command is supported on transceiver based stacking 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,
-> show stacking interfaces counters
1/52,
  InOctets      =            108040828,  OutOctets      =              4065016,
  InUcastPkts   =                89957,  OutUcastPkts   =                48056,
  InMcastPkts   =                   12,  OutMcastPkts   =                  868,
  InBcastPkts   =                    0,  OutBcastPkts   =                 2006,
  InPauseFrames =                    0,  OutPauseFrames =                    0,
  Sampling Interval 5 seconds
  InPkts/s      =                   28,  OutPkts/s      =                   16,
  InBits/s      =               268016,  OutBits/s      =                 9720
 4/27,
  InOctets      =              4012826,  OutOctets      =            108129633,
  InUcastPkts   =                48045,  OutUcastPkts   =                89945,
  InMcastPkts   =                  868,  OutMcastPkts   =                   12,
  InBcastPkts   =                 2006,  OutBcastPkts   =                    0,
  InPauseFrames =                    0,  OutPauseFrames =                    0,
  Sampling Interval 5 seconds
  InPkts/s      =                   16,  OutPkts/s      =                   29,
  InBits/s      =                 9840,  OutBits/s      =                270352

,
```

output definitions

InOctets	Number of octets received.
OutOctets	Number of octets transmitted.
InUcastPkts	Number of unicast packets received.
OutUcastPkts	Number of unicast packets transmitted.
InMcastPkts	Number of multicast packets received.
OutMcastPkts	Number of unicast packets transmitted.
InBcastPkts	Number of broadcast packets received.
OutBcastPkts	Number of unicast packets transmitted.
InPauseFrames	Number of MAC control frames received.
OutPauseFrames	Number of MAC control frames transmitted.

Release History

Release 6.6.1; command introduced.

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
healthPortTable
   healthPortTxLatest
   healthPortTx1MinAvg
   healthPortTx1HrAvg
   healthPortTx1HrMax
```

show interfaces counters errors

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

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

Syntax Definitions

stacking	Displays information for stacking ports.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, counter error information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number (for example, 3).
- These counters do not apply to Gigabit Ethernet traffic.
- For combo ports configured as either forced fiber or preferred fiber, statistics for the SFP fiber ports and not the copper RJ-45 ports is displayed. See the **show interfaces hybrid counters errors** command for more information.
- For combo ports configured as either forced copper or preferred copper, statistics for the copper RJ-45 ports and not the SFP fiber port is displayed. See the **show interfaces hybrid counters errors** command for more information.
- This command is supported on transceiver based stacking ports.

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
-> show stacking interfaces counters errors
1/52,
  IfInErrors        =                   0,
  Undersize pkts    =                   0,  Oversize pkts =                   0
 4/27,
  IfInErrors        =                   0,
  Undersize pkts    =                   0,  Oversize pkts =                   0
```

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 6.6.1; command 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***[/***port***[-***port2***]]] collisions**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, collision information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number (for example, 3).
- These counters do not apply to Gigabit Ethernet traffic.
- For combo ports configured as either forced fiber or preferred fiber, statistics for the SFP fiber ports and not the copper RJ-45 ports is displayed. See the **show interfaces hybrid collisions** command for more information.
- For combo port configured as either forced copper or preferred copper, statistics for the copper RJ-45 ports and not the SFP fiber port is displayed. See the **show interfaces hybrid collisions** command for more information.

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.

output definitions (continued)

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 6.6.1; command introduced.

Related Commands

interfaces tdr-test-start	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 [stacking] interfaces [*slot***[/***port***[-***port2***]]] status**

Syntax Definitions

stacking	Displays information for stacking ports.
slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, line settings for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number (for example, 3).
- The **show interfaces status** command displays the status and configuration of the active port in the first row and the status and configuration of the other port in the following row. See the **show interfaces hybrid status** command for more information.
- The hybrid mode for combo ports is not configurable; combo ports are set to preferred fiber by default. As a result, the Hybrid Mode field always displays preferred fiber (**PF**) for all combo ports. For non-combo ports, the Hybrid Type and Hybrid Mode fields display **NA**.
- This command is supported on transceiver based stacking ports.

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 1/25 status
                        DETECTED           CONFIGURED
Slot/ AutoNego  Speed Duplex Hybrid  Speed   Duplex Hybrid  Trap
Port           (Mbps)         Type   (Mbps)         Mode   LinkUpDown
-----+--------+------+------+------+--------+------+------+------
 1/25  Enable    -      -      -        1000  Full    PF   Enable
 1/25  Enable    -      -      -         100  Auto    PF   Enable

FF - ForcedFiber PF - PreferredFiber  F - Fiber
FC - ForcedCopper PC - PreferredCopper C - Copper
-> show stacking interfaces status
Slot/ AutoNego  Speed  Duplex
Port            (Mbps)
-----+--------+-------+--------
  1/51   -        -      -
  1/52   -      10000    Full
  4/27   -      10000    Full
  4/28   -        -      -
```

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 Mode	The configured combo port type, which is **PF** (Preferred Fiber). Configuring the Hybrid Mode is not supported.
Trap Link Up/Down	Trap Link status (up/down).

Release History

Release 6.6.1; command 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 clear-violation-all	Configures one or more combo ports to use the fiber SFP ports instead of the equivalent copper RJ-45 ports 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 (up or down), link status, violations, recovery time, maximum recovery attempts, along with the reason for violation in case link status of port is down 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	Slot number you want to display.
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 6450, 6350

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 is displayed. See the **show interfaces hybrid port** command for more information.

Examples

```
-> show interfaces 1/1 port
Legends: WTR – Wait To Restore
         #   - WTR Timer is Running & Port is in wait-to-restore state
Slot/    Admin     Link    Violations   WTR       Alias
Port     Status   Status               (sec)
-----+----------+---------+-----------+-----+-----------------
 1/1    enable      down    LinkMon        0 ""

-> show interfaces 1/1-3 port
Legends: WTR – Wait To Restore
         #   - WTR Timer is Running & Port is in wait-to-restore state
Slot/    Admin     Link    Violations   WTR       Alias
Port     Status   Status               (sec)
-----+----------+---------+-----------+-----+-----------------
 1/1    enable      down    LinkMon        0        ""
 1/2    enable      down    none         #10        ""
 1/3    enable      up      none          30        ""
```

```
-> show interfaces 1 port
Legends: WTR – Wait To Restore
         #   - WTR Timer is Running & Port is in wait-to-restore state
Slot/    Admin     Link    Violations    WTR          Alias
Port     Status   Status (sec)
-----+----------+---------+-----------+--------+-----------------
 1/1    enable      down    LFP        0           ""
 1/2    enable      down    none     #10           ""
 1/3    enable      up      none      20           ""
  .
  .
  .
 1/24   enable      up      none      30           ""
```

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.
Alias	Interface alias. Configured through the **interfaces alias** command.

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces admin	Enables/disables an interface.
interfaces clear-violation-all	Clears all port violations set by various applications on the switch.
interfaces alias	Configures an alias for a port.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortViolationBitMap
ifXTable
   ifAdminStatus
   ifOperStatus
   ifAlias
```

```
alaPortViolationRecoveryTable
   alaPortViolationRecoveryTime
   alaPortViolationRecoveryMaximum
```

show interfaces ifg

Displays interface inter-frame gap values.

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, IFG values for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number (for example, 3).

Examples

```
-> show interfaces ifg
 Slot/Port   ifg(Bytes)
-----------+-------------
 02/01          12
 02/02          12
 02/03          12
 02/04          12
 02/05          12
 02/06          12
 02/07          12
 02/08          12
 02/09          12
 02/10          12
 02/11          12
 02/12          12
 02/13          12
 02/14          12
 02/15          12
 02/16          12
 02/17          12
 02/18          12
```

output definitions

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

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces ifg	Configures the inter-frame gap value.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortCfgIFG
```

show interfaces flood rate

Displays configured flood rate settings.

show interfaces [*slot***[/***port***[-***port2***]]] flood rate [broadcast | multicast | unknown-unicast]**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, peak rate settings for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number.
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number only.

Examples

```
-> show interfaces 4 flood rate

Slot/  Bcast Bcast   Bcast    Ucast  Ucast   Ucast  Mcast   Mcast     Mcast
Port   Value Type    Status   Value  Type    Status Value   Type      Status
-----+---------+----+-------+----------+-----+-------+----------+-----+--------
4/1    496   mbps    enable   496    mbps    enable   496   mbps     disable
4/2     49   mbps    enable    49    mbps    enable    49   mbps     disable
4/3     49   mbps    enable    49    mbps    enable    49   mbps     disable
4/4     49   mbps    enable    49    mbps    enable    49   mbps     disable
4/5     49   mbps    enable    49    mbps    enable    49   mbps     disable
4/6     49   mbps    enable    49    mbps    enable    49   mbps     disable
4/7    496   mbps    enable   496    mbps    enable   496   mbps     disable
4/8    496   mbps    enable   496    mbps    enable   496   mbps     disable
4/9     49   mbps    enable    49    mbps    enable    49   mbps     disable
4/10    49   mbps    enable    49    mbps    enable    49   mbps     disable
```

Release History

Release 6.6.4; command introduced.

Related Commands

interfaces flood rate	Configures the rate limit based on storm type. The measurement unit for rate limit is Mbps, PPS and percentage.
interfaces flood enable	Enables or disables flood rate limiting for multicast traffic on an interface.

MIB Objects

```
esmConfTable
   esmPortMaxFloodRate
   esmPortMaxUnknownUcastFloodRate
   esmPortMaxMcastFloodRate
   esmPortFloodMcastEnable
   esmPortFloodBcastEnable
   esmPortFloodUnknownUcastEnable
```

show interfaces traffic

Displays interface traffic statistics.

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, traffic settings for all slots/ports on the switch are displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display all interfaces in a slot by entering the slot number (for example, 3).

Examples

```
-> show interfaces traffic

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

02/01                0                0         0                0
02/02                0                0         0                0
02/03                0                0         0                0
03/01                0                0         0                0
03/02                0                0         0                0
```

output definitions

Slot/Port	Interface slot and port numbers.
Input packets	Input packets detected.
Input bytes	Input bytes detected.
Output packets	Output packets detected.
Output bytes	Output bytes detected.

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces tdr-test-start	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 or transmitted).

MIB Objects

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

show interfaces hybrid

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

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that the status of the SFP ports is displayed.
copper	Specifies that the status of the copper RJ-45 ports is displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If no slot/port numbers are entered, information for all slots/ports on the switch is displayed.
- You can display a specific interface by entering the slot and port number (for example, 3/1).
- You can display a range of port numbers (for example, 3/1-4).
- You can display all interfaces in a slot by entering the slot number (for example, 3).

Examples

```
-> show interfaces 1/25 hybrid fiber
 Slot/Port  1/25 :
  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 autonegotiation 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 r oversized frames received.

output definitions (continued)

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 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 6.6.1; command 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 or 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 or 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***[***/port***[-***port2***]]] hybrid {fiber |copper} status**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that the status of the SFP ports is displayed.
copper	Specifies that the status of the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the status and configuration for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the *slot*, *slot/port*, or *slot/port-port2* parameters to display the status and configuration for all ports on a slot, a specific port, or a range of ports.
- The hybrid mode for combo ports is not configurable; combo ports are set to preferred fiber by default. As a result, the Hybrid Mode field always displays preferred fiber (**PF**) for all combo ports.

Examples

```
-> show interfaces hybrid fiber status
                        DETECTED           CONFIGURED
Slot/ AutoNego  Speed Duplex Hybrid  Speed   Duplex Hybrid  Trap
Port           (Mbps)         Type   (Mbps)         Mode   LinkUpDown
-----+--------+------+------+------+--------+------+------+------
 1/25  Enable    -      -      -        1000  Full    PF      -
 1/26  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).

output definitions (continued)

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 Mode	The configured combo port type, which is **PF** (Preferred Fiber). Configuring the Hybrid Mode is not supported.
Trap Link Up/Down	Trap Link status (up/down).

Release History

Release 6.6.1; command 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 clear-violation-all	Configures one or more combo ports to use the fiber SFP ports instead of the equivalent copper RJ-45 ports 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 flow control

Displays interface flow control wait time settings for combo ports.

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that the configuration of the SFP ports is displayed.
copper	Specifies that the configuration of the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the flow control wait time settings for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use the *slot*, *slot/port*, or *slot/port-port2* parameters to display the flow control wait time settings for all ports on a slot, a specific port, or for a range of ports.

Examples

```
-> show interfaces hybrid fiber flow control
 Slot/Port   Active  Wait time(usec) Cfg-Flow   Cfg-Cross
-----------+--------+---------------+--------+-----------
    1/25        -               0      Pause       MDI
    1/26        -               0      Pause       MDI
```

output definitions

Slot/Port	Interface slot and port number
Active	Interface status.
Wait time	Flow control wait time, in microseconds.
Cfg-Flow	Flow control status, which can be **Pause** or **Go**.
Cfg-Cross	The user-configured cross-over setting, which can be **Auto**, **MDI**, or **MDIX**.

Release History

Release 6.6.1; command introduced.

Related Commands

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

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIfIndex
esmHybridConfTable
   esmHybridPortCfgFlow
   esmHybridPortPauseSlotTime
   esmHybridPortCfgCrossover
```

show interfaces hybrid pause

Displays the flow control pause configuration for combo ports.

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that the configuration of the SFP ports is displayed.
copper	Specifies that the configuration of the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the flow control pause configuration for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces hybrid fiber pause
 Slot/Port   Active  Wait time(usec) Cfg-Pause  Cfg-Cross Hybrid Type
-----------+--------+---------------+--------+-----------+-----------
    1/25        -               0       DIS         MDI         -
    1/26        -               0       DIS         MDI         -

-> show interfaces hybrid copper pause
 Slot/Port   Active  Wait time(usec) Cfg-Pause  Cfg-Cross Hybrid Type
-----------+--------+---------------+--------+-----------+-----------
    1/25        -               0       DIS        Auto         -
    1/26     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 waits after receiving a PAUSE frame from the local interface.

output definitions (continued)

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 6.6.1; command 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 autonegotiation, 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***[/***port***[-***port2***]]] hybrid {fiber |copper} capability**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that the configuration of the SFP ports is displayed.
copper	Specifies that the configuration of the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the information for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Enter a slot and port number or a range of port numbers to display information for a specific combo port or a range of combo ports.
- Enter a slot number to display information for all combo ports on a specific slot.
- The **show interfaces hybrid capability** 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.

Examples

```
-> show interfaces 1/25 hybrid copper capability
   Slot/Port   AutoNeg     Flow   Crossover      Speed    Duplex
-----------+---------+--------+-----------+----------+----------
  1/25 CAP     EN/DIS   EN/DIS  MDI/X/Auto  10/100/1G  Full/Half
  1/25 DEF         EN       EN        Auto       Auto       Auto
```

output definitions

Slot	The slot number.
Port	The port number

output definitions (continued)

AutoNeg	In the row labeled **CAP** this field displays the valid autonegotiation configurations for the port. In the row label **DEF** this field displays the default autonegotiation 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**, **1 G**, **10/100/1 G**, 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 6.6.1; command introduced.

Related Commands

interfaces hybrid autoneg	Enables and disables autonegotiation 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***[/***port***[-***port2***]]] hybrid {fiber |copper} accounting**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that statistics for the SFP ports is displayed.
copper	Specifies that statistics for the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the accounting information for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces 1/25 hybrid copper accounting
1/25 ,
     Rx undersize packets         =                    0,
     Tx undersize packets         =                    0,
     Rx oversize packets          =                    0,
     Tx oversize packets          =                    0,
     Rx packets 64 Octets         =              3073753,
     Rx packets 65To127 Octets    =               678698,
     Rx packets 128To255 Octets   =                21616,
     Rx packets 256To511 Octets   =                21062,
     Rx packets 512To1023 Octets  =                    2,
     Rx packets 1024To1518 Octets =                   84,
     Rx packets 1519to4095 Octets =                    0,
     Rx packets 4096ToMax Octets  =                    0,
     Rx Jabber frames             =                    0
```

output definitions

Rx undersize packets	Number of undersized packets received.
Tx undersize packets	Number of undersized packets transmitted.
Rx oversize packets	Number of oversized packets received.
Tx oversize packets	Number of oversized packets transmitted.
Rx packets Octets	Number of packets received in each listed octet range.
Rx Jabber frames	Number of jabber packets received (longer than 1518 octets).
Tx deferred frames	Number of packets for which transmission was delayed (Ethernet only).

Release History

Release 6.6.1; command introduced.

Related Commands

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

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that statistics for the SFP ports is displayed.
copper	Specifies that statistics for the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the interface counters for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces 1/25 hybrid copper counters

InOctets      = 54367578586897979,  OutOctets     = 5.78E19,
InUcastPkts   = 55654265276,        OutUcastPkts  = 5.78E20,
InMcastPkts   = 58767867868768777,  OutMcastPkts  = 5465758756856,
InBcastPkts   = 576567567567567576, OutBcastPkts  = 786876,
InPauseFrames = 567798768768767,    OutPauseFrames= 786876,
```

output definitions

InOctets	Number of octets received.
OutOctets	Number of octets transmitted.
InUcastPkts	Number of unicast packets received.
OutUcastPkts	Number of unicast packets transmitted.
InMcastPkts	Number of multicast packets received.
OutMcastPkts	Number of unicast packets transmitted.

output definitions (continued)

InBcastPkts	Number of broadcast packets received.
OutBcastPkts	Number of unicast packets transmitted.
InPauseFrames	Number of MAC control frames received.
OutPauseFrames	Number of MAC control frames transmitted.

Release History

Release 6.6.1; command 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***[/***port***[-***port2***]]] hybrid {fiber |copper} counters errors**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that statistics for the SFP ports is displayed.
copper	Specifies that statistics for the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the error frame information for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces 1/25 hybrid copper counters errors

01/25,
  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 6.6.1; command 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***[/***port***[-***port2***]]] hybrid {fiber |copper} collisions**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that statistics for the SFP ports is displayed.
copper	Specifies that statistics for the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the information for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces 1/25 hybrid copper collisions

01/25,
  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 6.6.1; command 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***[/***port***[-***port2***]]] hybrid {fiber |copper} traffic**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that statistics for the SFP ports is displayed.
copper	Specifies that statistics for the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the traffic statistics for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces hybrid fiber traffic

Slot/Port   Input packets     Input bytes      Output packets    Output bytes
---------+-----------------+-----------------+-----------------+-----------------
01/25                  0                         0                 0
01/26                  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 6.6.1; command 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***[/***port***[-***port2***]]] hybrid {fiber |copper} port**

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that the status of the SFP ports is displayed.
copper	Specifies that the status of the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the port status for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces 1/25 hybrid fiber port
Slot/Port   Admin Status   Link Status                    Alias
----------+--------------+------------+-----------------------------------------
  1/25          enable          down     ""
```

output definitions

Slot/Port	Interface slot and port number.
Admin Status	Port status (enable/disable).
Link Status	Operational status (enable/disable).
Alias	Interface alias.

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces admin	Enables/disables an interface.
interfaces alias	Configures an alias for a port.

MIB Objects

```
esmConfTable
   esmPortCfgSlot
   esmPortCfgIfIndex
ifXTable
   ifAlias
ifTable
   ifAdminStatus
   ifOperStatus
```

show interfaces hybrid flood rate

Displays interface peak flood rate settings for combo ports.

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that the status of the SFP ports is displayed.
copper	Specifies that the status of the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the peak rate settings for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces flood rate

 Slot/Port   peak rate(Mb/second)   Enable
-----------+----------------------+---------------
 02/01            12                Flood only
 02/02            47                Flood only
 02/03            16                Flood only
 02/04            47                Flood only
 02/05            47                Flood only
 02/06            47                Flood only
 02/07            47                Flood only
 02/08            47                Flood only
 02/09            47                Flood only
 02/10            47                Flood only
 02/11            47                Flood only
 02/12            47                Flood only
 02/13            47                Flood only
 02/14            47                Flood only
 02/15            47                Flood only
 02/16            47                Flood only
 02/17            47                Flood only
```

```
02/18           47              Flood only
02/19           47              Flood only
```

output definitions

Slot/Port	Interface slot and port numbers.
Peak Rate (Mbps)	Configured peak flood rate.
Enable	Configuration enabled (Flood only/Flood Multicast/Multicast).

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces flood rate	Configures the rate limit based on storm type. The measurement unit for rate limit is Mbps, PPS and percentage.
interfaces flood enable	Enables/disables flood multicasting on an interface.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortMaxFloodRate
   esmPortFloodMcastEnable
```

show interfaces hybrid ifg

Displays interface inter-frame gap values for combo ports.

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

Syntax Definitions

slot	Slot number you want to display.
port	Port number of the interface you want to display.
port2	Last port number in a range of ports you want to display.
fiber	Specifies that statistics for the SFP ports is displayed.
copper	Specifies that statistics for the copper RJ-45 ports is displayed.

Defaults

If a specific slot or slot/port number is not entered with this command, the inter-frame gap values for all switch combo ports is displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

```
-> show interfaces hybrid fiber ifg
 Slot/Port   ifg(Bytes)
-----------+-------------
  1/25          12
  1/26          12
```

output definitions

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

Release History

Release 6.6.1; command introduced.

Related Commands

interfaces ifg	Configures the inter-frame gap value.

MIB Objects

```
esmConfTable
   esmPortSlot
   esmPortIF
   esmPortCfgIFG
```

interfaces violation-recovery-time

Configures the time interval after which the port is automatically reactivated if the port was shut down for any violation. Recovery timer 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 secs. 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 6450, 6350

Usage Guidelines

- When the recovery timer expires, the interface is operationally re-enabled, and the violation on the interface is cleared.
- The violation recovery timer 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 6.6.3; 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 6450, 6350

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 secs (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 6.6.3; command introduced.

Related Commands

interfaces violation-recovery-time	Configures the time interval after which the port is automatically reactivated 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 6450, 6350

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 6.6.3; command introduced.

Related Commands

interfaces violation-recovery-time	Configures the time interval to automatically re-enable the ports that were shut down 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 6450, 6350

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 6.6.3; command introduced.

Related Commands

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

MIB Objects

```
esmConfTable
   esmPortViolationClearAll
```

show interfaces violation-recovery

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

show interfaces violation-recovery

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

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

output definitions

UserPorts Shutdown Recovery Time	The recovery time configured.
UserPorts Shutdown Recovery Trap	SNMP recovery trap status: Enable or Disable.
UserPorts Shutdown Maximum Recovery	The maximum recovery attempts configured for the port before a port is permanently shut down.

Release History

Release 6.6.3; command introduced.

Related Commands

interfaces violation-recovery-time	Configures the time interval after which the port is automatically reactivated 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
```

link-fault-propagation group

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

link-fault-propagation group *num*

no link-fault-propagation group *num*

Syntax Definitions

num	Indicates the unique group ID. The allowed range is 1-8.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

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

Examples

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

Release History

Release 6.7.2.R02; 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.
link-fault-propagation group admin-status	Allows to administratively enable or disable link-fault-propagation on a group or groups.

MIB Objects

```
alaLFPGroupTable
   alaLFPGroupId
   alaLFPGroupRowStatus
```

link-fault-propagation group admin-status

Allows to administratively enable or disable Link Fault Propagation on a group.

link-fault-propagation group *num* **admin-status {enable | disable}**

Syntax Definitions

num	Indicates the unique group ID. The allowed range is 1-8.

Defaults

By default, the admin status of a group is disabled.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Admin status option is available when a LFP group is created.

Examples

```
-> link-fault-propagation group 1 admin-status enable
-> link-fault-propagation group 1 admin-status disable
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

link-fault-propagation group	Configures a Link Fault Propagation (LFP) group to associate with source and destination ports.
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
   alaLFPGroupAdminStatus
   alaLFPGroupRowStatus
```

link-fault-propagation group source

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

link-fault-propagation group *num* **source {port** *slot/port* **[**-*port2***] | linkagg** *aggid* **[**-*aggid2***]}**

no link-fault-propagation group *num* **source {port** *slot/port* **[**-*port2***] | linkagg** *aggid* **[**-*aggid2***]}**

Syntax Definitions

num	An existing LFP group ID number. The valid range is 1–8.
slot/port **[**-*port2***]**	The slot number for the module and the physical port number on that module (e.g. 2/1 specifies port 1 on slot 2). *port2* refers to the last port in the range of ports.
aggid **[**-*aggid2***]**	Link Aggregate Identifier. *aggid2* refers to the last aggregate identified in the range of aggregates.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 maximum of 32 link aggregates will be supported irrespective of the number of ports in the each aggregate in a group.
- A Maximum 48 source/destination ports shall be supported in a group. The ports can be physical ports or link aggregates.
- A port or linkagg added as a source port in a group cannot be added as a destination port for this group or in any other group.
- A port or linkagg added as a destination port in a group cannot be added as a source port for this group or in any other group.
- If port is recovered due to interface recovery timer, then the port will go back to the shutdown state if the error persists.

Examples

```
-> 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 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
-> no link-fault-propagation group 1 source linkagg 3 destination linkagg 1
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

link-fault-propagation group	Configures a Link Fault Propagation (LFP) group to associate with source and destination ports.
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
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 *num* **destination {port** *slot/port[-port2]* **| linkagg** *agg_id[-agg_id2]***}**

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

Syntax Definitions

num	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 6450, 6350

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 32 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 6.7.2.R02; 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 duration of time after all the source ports go down that LFP waits before shutting down the destination ports.

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

Syntax Definitions

num	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 6450, 6350

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.

Examples

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

Release History

Release 6.7.2.R02; command introduced.

Related Commands

link-fault-propagation group	Configures a Link Fault Propagation (LFP) group to associate with source and destination ports.
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 details of a Link Fault Propagation group.

show link-fault-propagation group *num*

Syntax Definitions

num	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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> 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

-> 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
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

link-fault-propagation group	Creates or deletes a link fault propagation group.
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.

MIB Objects

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

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 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 6450, 6350

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.
- DDM information will be displayed for all the ports irrespective of the operational status of the port, either remote or local.
- Whenever the values goes off the scale value, they will be represented as **Inf** or **NaN** in the show output. Monitoring the transceivers with the help of DDM prevents the device from getting damaged due to high operational values.

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 DDM trap status: enable or disable.
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 6.6.4; command was introduced.
Release 6.7.2.R02; **DDM Trap Status** field added.

Related Commands

interfaces transceiver ddm	Configures the DDM administrative status.

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
ddmInfoEntry
ddmConfigGroup
ddmInfoGroup
ddmInfoTable
ddmInfoEntry
ddmConfig
ddmTrapConfig
```

show interfaces eee

Displays the EEE capability on the specified ports.

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

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).
eee	Displays the EEE capability on the specified ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- For fiber ports NA will be displayed.
- A capability of 100M/1000M signifies that port is capable of EEE on both 100M and 1000M speeds.
- Autonegotiation is the current link speed on which the EEE is working.
- EEE is not supported on a port operating at 10M speed. Autonegotiation will display '-'.

Examples

```
show interfaces 1 eee

-> show interfaces eee
 Slot/    Status    Capability    Autonegotiation
 Port

--------+---------+-------------+-----------------
  1/1    disable   100M/1000M          -
  1/2    enable    100M/1000M          1000M
  1/3    enable    100M/1000M          100M
  1/4    enable    100M/1000M          -
  1/5    disable   100M/1000M          -
  1/6    disable   100M/1000M          -
```

output definitions

Slot/Port	Interface slot and port numbers.
Status	Whether EEE is enabled or disabled.

output definitions (continued)

Capability	Signifies that port is capable of EEE on both 100M and 1000M speed
Autonegotiation	The current link speed on which EEE is operating.

Release History

Release 6.6.4; command was introduced.

Related Commands

interfaces eee	Enables or disabled Energy Efficient Ethernet.

MIB Objects

```
esmConfTable
   esmPortCfgEeeStatus
   esmPortCfgEeeAutoNegState
   esmPortCfgEeeCapapbility
```

show interfaces ptp

Displays the current IEEE 1588 Precision Time Protocol (PTP) status on the switch. When PTP is enabled, the switch provides IEEE 1588 support.

show interfaces ptp

Syntax Definitions

N/A

Defaults

By default, IEEE 1588 Precision Time Protocol (PTP) is disabled.

Platforms Supported

OmniSwitch 6450 (OS6450-P10S and OS6450-U24S only)

Usage Guidelines

N/A

Examples

```
-> show interfaces ptp

PTP Status      : enable
```

Release History

Release 6.6.5; command was introduced.

Related Commands

interfaces ptp	Enables or disables IEEE 1588 Precision Time Protocol (PTP) on the switch.
show interfaces ptp-statistics	Displays IEEE 1588 Precision Time Protocol (PTP) ingress and egress statistics for each port.

MIB Objects

```
WRPesmShowInterfacesPtp
```

show interfaces ptp-statistics

Displays IEEE 1588 Precision Time Protocol (PTP) ingress and egress statistics for each port.

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

Syntax Definitions

slot	The slot number for a specific module.
slot/*port***[-***port2***]**	The slot and port number (1/6). Use a hyphen to specify a range of ports (1/6-1/10).
ptp-statistics	Displays the PTP statistics on the specified ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6450 (OS6450-P10S and OS6450-U24S only)

Usage Guidelines

If PTP is disabled, an error displays when entering this command. To enable PTP, use the **interfaces ptp** command.

Examples

```
-> show interfaces ptp-statistics
 Slot/     Ingress       Ingress        Ingress        Ingress        Egress        Egress        Egress        Egress
 Port      PTPV2         PTPV1          Drop           piggy_back     PTPV2         PTPV1         Drop          Update_res
---------+-------------+--------------+--------------+--------------+-------------+-------------+-------------+--------------
  1/1      2761156       0              0              574017         1286446       0             0             1282435
  1/2      257315        0              0              256514         3456655       0             0             1469152
  1/3      257322        0              0              256521         3456658       0             0             1469148
  1/4      257322        0              0              256521         3456703       0             0             1469167
  1/5      1027309       0              0              256660         257344        0             0             256543
  1/6      0             0              0              0              0             0             0             0
  1/7      0             0              0              0              5797545       0             0             1940125
  1/8      0             0              0              0              0             0             0             0
  1/9      257250        0              0              256449         3457222       0             0             1469419
  1/10     514932        0              0              513324         4485249       0             0             1726206
```

output definitions

Slot/Port	Interface slot and port numbers.
Ingress PTPV2	The number of PTP V2 packets ingressing the port.
Ingress PTPV1	The number of PTP V1 packets ingressing the port.
Ingress Drop	The number of PTP packets dropped at ingress by the port.
Ingress piggy_back	The number of PTP (ingress) packets timestamped at ingress (piggy back mode) in the port.
Egress PTPV2	The number of PTP V2 packets egressing the port.
Egress PTPV1	The number of PTP V1 packets egressing the port.

output definitions (continued)

Egress Drop	The number of PTP packets dropped at egress by the port.
Egress Update_res	The number of PTP packets in which residence times were updated when egressing port.

Release History

Release 6.6.5; command was introduced.

Related Commands

interfaces ptp	Enables or disables IEEE 1588 Precision Time Protocol (PTP) on the switch.
show interfaces ptp	Displays the current IEEE 1588 Precision Time Protocol (PTP) status on the switch.

MIB Objects

```
WRPesmShowStatisticsPtp
EsmPtpStatsEntry
esmPtpStatsTable
   esmPtpStatsIngPtpv2
   esmPtpStatsIngPtpv1
   esmPtpStatsIngPtpDrop
   esmPtpStatsIngPtpPigBag
   esmPtpStatsEgrPtpv2
   esmPtpStatsEgrPtpv1
   esmPtpStatsEgrPtpDrop
   esmPtpStatsEgrPtpUpdateRes
```

24 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 mac
vlan mac range
vlan ip
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 6450, 6350

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 6.6.1; 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 6450, 6350

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.

- MAC address rules and protocol rules also capture DHCP client traffic.
- 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 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 6450, 6350

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 24-12).
- 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 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 | decnet | appletalk | ethertype** *type* **| dsapssap** *dsap/ssap* **| snap** *snap-type***}**

vlan *vid* **no protocol {ip-e2 | ip-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.
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 6450, 6350

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, 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 protocol rules, a message displays recommending the use of the IP 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 30 protocol ethertype 0600
-> vlan 40 protocol dsapssap F0/F0
-> vlan 50 protocol snap 6004
-> vlan 10 no protocol ip-snap
-> vlan 30 no protocol ethertype 0806
-> vlan 40 no protocol dsapssap 04/04
-> vlan 50 no protocol snap 80FE
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 IP and Appletalk traffic and VLAN 10 has an IP protocol rule and VLAN 20 has an appletalk 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; command was introduced.
Release 6.6.2; command was deprecated.

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 6450, 6350

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 6.6.1; 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 6450, 6350

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
  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
  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 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 6.6.1; 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).

MIB Objects

N/A

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 6450, 6350

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-8021x   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-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 6.6.1; command was introduced.

Related Commands

show vlan port	Displays VLAN port assignments for all VLANs, a specific VLAN, or for a specific port.

MIB Objects

N/A

25 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 port default
vlan source-learning
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 *vid* **[enable | disable] [name** *description***]**

no vlan *vid*

Syntax Definitions

vid	A numeric value (2–4094) that uniquely identifies an individual VLAN. This value becomes the VLAN ID for the new VLAN.
description	Text string up to 32 characters. Use quotes around string if description contains multiple words with spaces between them (for example, “Alcatel Marketing VLAN”).
enable	Enable VLAN administrative status.
disable	Disable VLAN administrative status.

Defaults

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

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

vlan port default	Statically assigns ports to a VLAN.
show vlan	Displays a list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanAdmStatus
   vlanOperStatus
   vlanStatus
```

vlan stp

Enables or disables the Spanning Tree status for a VLAN.

vlan *vid* **[1x1 | flat] stp {enable | disable}**

Syntax Definitions

vid	A VLAN ID number (1–4094).
1x1	Specifies that the Spanning Tree status for the VLAN applies when the switch is running in the 1x1 Spanning Tree mode.
flat	Specifies that the Spanning Tree status for the VLAN applies when the switch is running in the flat Spanning Tree mode.
enable	Enables Spanning Tree for the specified VLAN.
disable	Disables Spanning Tree for the specified VLAN.

Defaults

By default, the Spanning Tree status is enabled in both the 1x1 and flat mode when the VLAN is created.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

vlan	Creates a VLAN.
bridge mode	Selects a flat Spanning Tree or 1x1 Spanning Tree operating mode for a switch.
show vlan	Displays a list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanStpStatus
   vlan1x1StpStatus
   vlanflatStpStatus
```

vlan mobile-tag

Enables or disables classification of tagged packets received on mobile ports. If a mobile port receives a tagged packet with a VLAN ID that matches the specified VLAN ID, the port and packet are dynamically assigned to that VLAN. If vlan mobile-tag is disabled, the packets tagged with a VLAN ID that does not match the mobile port's default VLAN or a rule VLAN that the traffic qualifies for, the packet is dropped.

vlan *vid* **mobile-tag {enable | disable}**

Syntax Definitions

vid	An existing VLAN ID number (1–4094).
enable	Enables dynamic assignment of tagged mobile port packets to the specified VLAN.
disable	Disables dynamic assignment of tagged mobile port packets to the specified VLAN.

Defaults

By default, mobile port tagging is disabled when a VLAN is created.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

vlan	Creates a VLAN.
show vlan	Displays a list of existing VLANs.
show vlan port	Displays VLAN port assignments.

MIB Objects

```
vlanTable
   vlanNumber
   vlanTagMobilePortStatus
```

vlan 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_num***}**

vlan *vid* **no port default {***slot/port* | *link_agg_num***}**

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_num	The link aggregate ID number (0–31) to assign to the specified VLAN. See Chapter 12, "Link Aggregation Commands."

Defaults

VLAN 1 is the default VLAN for all ports.

Platforms Supported

OmniSwitch 6450, 6350

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.
- This command is also supported on an NNI interface.

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 6.6.1; command was introduced.
Release 6.6.5; command supported on NNI interface.

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***] | ipmvlan** *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 (for example, 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 6450, 6350

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 IPMVLAN 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 IPMVLAN.

Examples

```
-> vlan 10-15 source-learning disable
-> vlan ipmvlan 10 source-learning disable
```

Release History

Release 6.6.1; command was 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 configured on the switch.

show vlan [*vid***]**

Syntax Definitions

vid	VLAN ID number (1–4094).

Defaults

By default, a list of all VLANs is displayed.

Platforms Supported

OmniSwitch 6450, 6350

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.
- The MAC Tunneling status for the SVLAN is displayed only when the specific VLAN ID is mentioned in the command.

Examples

```
-> show vlan
                              stree                mble  src
vlan  type  admin  oper  1x1   flat auth   ip   tag   lrn     name
-----+-----+------+-----+----+-----+----+-----+ ----+-----+---------
 1    std   on     on     on    on   off   off  off    on     VLAN 1
100   vstk  on    off     off   on   off   off  off    off    VLAN 100
11    unp   on    off    off    on   off   off   off   on     VLAN 10

-> show vlan 1

Name                : VLAN 1,
Administrative State: enabled,
Operational State   : enabled,
1x1 Spanning Tree State : enabled,
Flat Spanning Tree State : enabled,
IP Router Port      : off,
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,
IP Router Port      : off,
IP MTU              : 1500,
Mobile Tag          : off,
Source Learning     : disabled,
Traffic-Type        : ethernet-service Customer SVLAN,
Priority-Map        : x->0
MAC Tunneling       : disabled,
```

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 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.
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). Note that this status is always **off** because configuring authenticated VLANs is not supported.
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.
name	The user-defined text description for the VLAN. By default, the VLAN ID is specified for the VLAN description.

output definitions (continued)

Traffic-Type	Type of traffic passing through the VLAN. For example, customer traffic tunneled through a VLAN Stacking Ethernet Service VLAN (SVLAN). Note this VLAN Stacking is supported only on Metro switches.
Priority-Map	Priority map value set for the VLAN.
MAC Tunneling	Displays the MAC tunneling status of the SVLAN.

Release History

Release 6.6.1; command was introduced.
Release 6.6.5; MAC Tunneling output field added.
Release 6.7.2; VLAN type **unpd** for UNP dynamic VLANS 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
   vlanTagMobilePortStatus
   vlanSvlanMacTunnelStatus
```

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). Also displays the entire VLAN membership for the NNI interface.

show vlan [*vid***] port [***slot/port* | *link_agg***]**

Syntax Definitions

vid	VLAN ID number (1–4094).
slot/port	Enter the slot number for the module and the physical port number on that module (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 6450, 6350

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.
- 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
  1/4   vstkQtag    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), vstkQtag (tagged 802.1q, QinQ, and untagged services using the same uplink NNI port) **mobile** (dynamic secondary VLAN assignment for the port), **mirror** (port is mirroring the VLAN assignment of another port), or **dynamic** (VPAs that are learned 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 6.6.1; command was introduced.
Release 6.6.5; vstkQtag option introduced

Related Commands

show vlan	Displays list of VLANs configured on the switch.
show vlan router mac status	Displays the current MAC router operating mode (single or multiple) and VLAN router 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 6450, 6350

Usage Guidelines

- Only single MAC router mode is supported at this tine, 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
----------------------+-------------+--------------+----------
       disabled               5              1           1
```

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 (IP). 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 6.6.1; 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
```

show vlan gvrp

Displays a list of VLANs learned through GVRP and their details.

show vlan gvrp [*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

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the *vlan-id* or *vlan-range* parameter with this command to display the details for a specific VLAN(s).

Examples

```
-> show vlan gvrp
                              stree                    mble
vlan  type  admin oper  1x1    flat    auth   ip    tag     name
----+-----+-----+----+-----+--------+-------+------+-----+--------------
 5   gvrp   on    on   on      on      off   NA    off    GVRP1
 6   gvrp   on    on   off     off     off   NA    off    GVRP12
```

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 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.
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 6.6.1; 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
   vlanTagMobilePortStatus
```

show vlan ipmvlan

Displays IPMVLAN information for a specific IPMVLAN, a range of IPMVLANs, or all the IPMVLANs.

show vlan ipmvlan [*ipmvlan-id* **|** *ipmvlan-id1-ipmvlan-id2***]**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number. The valid range is 2–4094.
ipmvlan-id1-ipmvlan-id2	Specifies the range of the IP Multicast VLAN numbers.

Defaults

By default, the details of all the IPMVLANs will be displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the *ipmvlan-id* parameter with this command to display details of a specific IPMVLAN.
- Use the *ipmvlan-id1-ipmvlan-id2* parameter with this command to display details of 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 6.6.1; 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
```

26 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; command was introduced.

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 6450

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 learned 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 learned earlier will be maintained.

Examples

```
-> gvrp maximum vlan 100
```

Release History

Release 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; command was introduced.

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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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
```

27 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 32-256.

Defaults

The default value is 256.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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 6450, 6350

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 6.6.5; command 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.
vlan-range	The VLAN ID range (For example, 1-10)

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
stree Flat	Specifies that the MVRP status for the VLAN applies when the switch is running in the flat MVRP mode.

output definitions (continued)

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 6.6.5; command 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 6450, 6350

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 6.6.5; command introduced.

Related Commands

show mvrp statistics	Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpGlobalClearStats
   alaMvrpPortStatsTable
   alaMvrpPortStatsClearStats
```

28 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.

Additionally, standard VLAN support on NNI ports' allows any standard (non-service) VLAN to be associated to NNI ports of type untagged or 8021q tagged. However, VLAN 1, cannot be associated as untagged member to a NNI port. 802.1q services, QinQ service and untagged services can be configured using the same uplink NNI port. This allows the customer to use an untagged management VLAN to manage the switch through NNI ports.

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** **ethernet-service mac-tunneling** **ethernet-service untagged-cvlan-insert** **ethernet-service sap uni untagged-cvlan** **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** **clear ethernet-service uni-profile l2pt-statistics** **show ethernet-service uni-profile l2pt- statistics** **show ethernet-service untagged-cvlan-insert**
Ethernet Service Hardware Loopback Test	**loopback-test** **show loopback-test**
Ethernet Service MAC-Tunneling	**ethernet-service mac-tunneling** **ethernet-service svlan mac-tunneling**

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 (for example, 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 (for example, “Alcatel 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 6450

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.
- Configure (tagged with standard VLAN) as NNI, using the command **ethernet-service svlan nni**.
- 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.
- If the default VLAN is removed from the NNI interface, then the default VLAN must be changed to 4095.
- It is not possible to configure VLAN 1 as default VLAN of an NNI interface.

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 for 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 6450

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 (for example, 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 6450

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 (for example, “Alcatel 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 6450

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 (for example, 10-12 specifies VLANs 10, 11, and 12).
slot/port1	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, 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 6450

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.
- Some restrictions on NNI interface are:
  - NNI interface cannot be a mobile port.

- NNI interface cannot be an aggregable port.
- NNI interface cannot be a destination mirroring port.

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 (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, 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 6450

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 (that is, 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.
- MVRP legacy BPDU are supported only on network ports that already have MVRP 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.
- An error message is displayed, if the user tries to configure TPID, other than 0x8100, on 802.1Q tagged NNI interface.

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 6450

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 (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, 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 6450

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 6450

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 (for example, “Alcatel 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 6450

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 6450

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 (for example, “Alcatel 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 6450

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

	peer	discard	tunnel
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

- 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.
- 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 (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, 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 (for example, “Alcatel 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 6450

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 6450

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

ethernet-service mac-tunneling	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
```

ethernet-service mac-tunneling

Configures the global mac-tunneling status.

ethernet-service mac-tunneling {enable | disable}

Syntax Definitions

enable	The mac-tunneling status is enabled globally.
disable	The mac-tunneling status is disabled globally.

Defaults

parameter	default
enable | disable	

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- When mac-tunneling is enabled globally, per SVLAN mac-tunneling configuration will not be active.
- When mac-tunneling is disabled globally, the MAC tunnel status of the SVLANs configured will be active.
- Any changes to the mac-tunneling status will be effective only on reload.

Examples

```
-> ethernet-service mac-tunneling enable
-> ethernet-service mac-tunneling disable
```

Release History

Release 6.6.5; command introduced.

Related Commands

ethernet-service svlan mac-tunneling	Configures the mac-tunneling status for SVLAN.

MIB Objects

```
alaEServiceL2MacTunnel
```

ethernet-service untagged-cvlan-insert

Configures the global status for CVLAN insertion for untagged packets.

ethernet-service untagged-cvlan-insert {enable | disable}

Syntax Definitions

enable	The CVLAN insertion for untagged packets is enabled.
disable	The CVLAN insertion for untagged packets is disabled.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use this command to enable CVLAN on untagged packets, before before specifying which CVLAN need to be added in all the incoming untagged frames on a specific uni port.
- Enabling **ethernet-service untagged-cvlan-insert** feature on the switch would imply that the existing legacy behavior of UNI and NNI ports will no longer hold good.

Examples

```
-> ethernet-service untagged-cvlan-insert enable
-> ethernet-service untagged-cvlan-insert disable
```

Release History

Release 6.6.5; command introduced.

Related Commands

ethernet-service sap uni untagged-cvlan	Specifies which CVLAN needs to be added in all the incoming untagged frames on a specific uni port.
show ethernet-service untagged-cvlan-insert	Displays the status of the CVLAN insertion for untagged packets

MIB Objects

```
alaEServiceUntaggedMode
```

ethernet-service sap uni untagged-cvlan

Specifies which CVLAN needs to be added in all the incoming untagged frames on a specific UNI port.

ethernet-service sap *sap_id* **uni {***slot/port* | **linkagg** *agg_num***}untagged-cvlan** *cvlan_id*

Syntax Definitions

sap_id	Specify the SAP ID number identifying the service instance.
cvlan_id	Specify the CVLAN that needs to be added inside the untagged frames for the frames that are incoming in this UNI.
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 link aggregate ID number (0–31).

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- This command will be accepted only when CVLAN on untagged feature is enabled. Use the command **ethernet-service untagged-cvlan-insert** to enable CVLAN on untagged feature.
- For a specific UNI, only one CVLAN can be mapped when CVLAN on untagged feature is enabled.

Examples

```
-> ethernet-service sap 10 uni 1/7 untagged-cvlan 10
-> ethernet-service sap 10 uni 1/9 untagged-cvlan 11
```

Release History

Release 6.6.5; command introduced.

Related Commands

ethernet-service untagged-cvlan-insert	Configures the global status for CVLAN insertion for untagged packets.
show ethernet-service untagged-cvlan-insert	Displays the status of the CVLAN insertion for untagged packets

MIB Objects

```
alaEServiceSapUniRowStatus
```

ethernet-service svlan mac-tunneling

Configures the mac-tunneling status for SVLAN.

ethernet-service svlan *svid1***[**-*svid2***] mac-tunneling {enable | disable} [***name description***]**

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 (for example, 10-12 specifies VLANs 10, 11, and 12).
enable	The mac-tunneling status is enabled globally.
disable	The mac-tunneling status is disabled globally.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- When mac-tunneling is enabled globally, per SVLAN mac-tunneling configuration will not be active.
- When mac-tunneling is disabled globally, the MAC tunnel status of the SVLANs configured will be active.
- Maximum four SVLAN can have MAC tunnel enabled simultaneously.
- Mac-tunneling must be disabled globally before mac-tunneling is enabled on per SVLAN.

Examples

```
-> ethernet-service svlan 1000 mac-tunneling enable name "VLAN 1000"
-> ethernet-service svlan 1000 mac-tunneling disable name "VLAN 1000"
```

Release History

Release 6.6.5; command introduced.

Related Commands

ethernet-service mac-tunneling	Configures the global mac-tunneling status.
show vlan	Displays a list of VLANs and their attributes configured on the switch.

MIB Objects

```
vlanTable
   vlanNumber
   vlanSvlanMacTunnelStatus
   vlanDescription
```

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 6450

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 6450

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 for 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 (for example, 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 6450

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 (for example, “Alcatel 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 6450

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 6450

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 (for example, 3/1 specifies port 1 on slot 3).
agg_num	The link aggregate ID number (0–31).

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 (for example, 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 6450

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 (for example, 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 6450

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 (for example, 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 6450

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 (for example, 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 6450

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 (for example, 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 6450

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 (for example, 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 6450

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 (for example, “Alcatel Engineering”).

Defaults

By default, all UNI profiles are displayed if a UNI profile name is not specified with this command.

Platforms Supported

OmniSwitch 6450

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

-> show ethernet-service uni-profile ieee-drop-all
 Profile Name: ieee-drop-all
 All IEEE Mac Addresses : 01:80:C2:00:00:00 - 01:80:c2:00:00:0f : drop

-> show ethernet-service uni-profile ieee-fwd-all
Profile Name: ieee-fwd-all
All IEEE Mac Addresses: 01:80:C2:00:00:00 - 01:80:c2:00:00:ff : tunnel,
Pause frame : 01:80:C2:00:00:01 : drop,
MAC specific control frame : 01:80:C2:00:00:04 : drop
```

output definitions

Profile Name	The name of the UNI profile.

output definitions

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 uni-profile l2pt- statistics

Displays the profile statistics for VLAN Stacking User Network Interface (UNI) profiles.

show ethernet-service uni-profile [*uni-profile-name***] l2pt-statistics**

Syntax Definitions

uni-profile-name	Alphanumeric string of up to 32 characters. Write string within quotes if the profile name contains multiple words with spaces between them, for example: “Alcatel Engineering”.

Defaults

By default, statistics of all UNI profiles are displayed if a UNI profile name is not specified with this command.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Specify a UNI profile name to display the statistics for a single UNI profile.

Examples

```
> show ethernet-service uni-profile l2pt-statistics
UNI Profile: Profile_1
Total RX:123456,
L2 Protocol:
STP
Rx:1234,
Hardware Action:CPU, 802.1x
Rx:1234,
Hardware Action:FWD, 802.3ad, OAM, LACPMARKER
Rx1234,
Hardware Action:CPU, 802.1ab
Rx1234,
Hardware Action:CPU,PAPG, UDLD, CDP, DTP, VTP, PVST, VLAN, UPLINK
Rx1234,
Hardware Action:CPU, GVRP, MVRP
Rx1234,
Hardware Action:DROP, AMAP
Rx1234,
Hardware Action:FWD,

UNI Profile: Profile_2
Total RX:18,
L2 Protocol:
STP
Rx:1234,
Hardware Action:CPU, 802.1x
Rx:1234,
```

```
Hardware Action:FWD, 802.3ad, OAM, LACPMARKER
Rx1234,
Hardware Action:CPU, 802.1ab
Rx1234,
Hardware Action:CPU, PAPG, UDLD, CDP, DTP, VTP, PVST, VLAN, UPLINK
Rx1234,
Hardware Action:CPU, GVRP, MVRP
Rx1234,
Hardware Action:DROP, AMAP
Rx1234,
Hardware Action:FWD,
Custom Protocol1 1234,
Hardware Action:FWD,
Custom Protocol2122,
Hardware Action:DROP
```

output definitions

UNI Profile	The UNI profile associated with the port.
STP	Spanning Tree Protocol.
RX	The total number of frames received by the protocol on the port and trapped in CPU.
Hardware Action	Displays the configured hardware action.
Custom Protocol	Displays the custom-L2-protocol associated to the UNI profile.

Release History

Release 6.6.4; command was introduced.

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-profile custom-L2-protocol	Associates a custom-L2-protocol entry to a UNI profile.
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

```
AlaEServiceUNIProfileL2ProtocolTotalStatisticsEntry
alaEServiceUNIProfile
alaEServiceUNIProfileL2ProtocolTotalRxFrames

AlaEServiceUNIProfileCustomL2ProtocolStatisticsEntry
alaEServiceUNIProfileCustomL2StatsProfileID,
alaEServiceUNIProfileCustomL2ProtocolIndex,
alaEServiceUNIProfileCustomL2ProtocolRxFrames,
alaEServiceUNIProfileCustomL2ProtocolTreatment

AlaEServiceUNIProfileCustomL2ProtocolStatisticsEntry
alaEServiceUNIProfileCustomL2StatsProfileID,
```

```
alaEServiceUNIProfileCustomL2ProtocolIndex,
alaEServiceUNIProfileCustomL2ProtocolRxFrames,
alaEServiceUNIProfileCustomL2ProtocolTreatment
```

show ethernet-service untagged-cvlan-insert

Displays the status of the CVLAN insertion for untagged packets.

show ethernet-service untagged-cvlan-insert

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show ethernet-service untagged-cvlan-insert
   Cvlan insertion for untagged packets : Enabled
```

output definitions

Enabled	Specifies that the CVLAN insertion for untagged packets support status is enabled.
Disabled	Specifies that the CVLAN insertion for untagged packets support status is disabled.

Release History

Release 6.6.5; command was introduced.

Related Commands

ethernet-service untagged-cvlan-insert	Configures the global status for CVLAN insertion for untagged packets.
ethernet-service sap uni untagged-cvlan	Specifies which CVLAN needs to be added in all the incoming untagged frames on a specific uni port.

MIB Objects

N/A

clear ethernet-service uni-profile l2pt-statistics

Clears the statistics of all UNI profile.

clear ethernet-service uni-profile [*uni profile name***] l2pt-statistics**

Syntax Definitions

uni-profile-name	Name of the uni-profile whose statistics has to be displayed. It is an alphanumeric string of up to 32 characters. Use string within quotes if the profile name contains multiple words with spaces between them, for example: “Alcatel Engineering”.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use an existing uni-profile name with the clear command.

Examples

```
-> clear ethernet-service uni-profile uni-profile 1 l2pt-statistics
```

Release History

Release 6.4.4; 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 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 (for example, “Alcatel Engineering”).

Defaults

By default, all SAP profiles are displayed if a SAP profile name is not specified with this command.

Platforms Supported

OmniSwitch 6450

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* **destination-mac** *dest_address* **loopback-port** *slot/port* **[source-mac** *src_address***] [vlan** *vlan_id***] type inward**

loopback-test *profile_name* **destination-mac** *dest_address* **loopback-port** *slot/port* **[source-mac** *src_address***] vlan** *vlan_id* **type outward [sap** *sap_id***]**

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 (for example, “Alcatel 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.
sap_id	The SAP ID in the range 1 to 1024.
enable	Enables the loopback test profile.
disable	Disables the loopback test profile.

Defaults

parameter	default
type	**inward**
vlan_id	0
src_address	00:00:00:00:00:00

Platforms Supported

OmniSwitch 6450

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.
- For inward loopback, it is mandatory to provide the destination MAC address and loopback port. The source MAC address and VLAN ID is optional.
- For outward loopback, it is mandatory to provide the destination MAC address, loopback port, and VLAN ID. The source MAC address is optional.
- When a loopback profile is configured without the source MAC address and VLAN ID, by default, its value is taken as '0'. The **show loopback-test** command will display the default value for source MAC address and VLAN as 'Any'.
- Loopback test must be manually restarted if the test is interrupted by a takeover, restart, or hot swap.
- Loopback test is not supported on link aggregation ports.
- 'loopback-test <*profile-name*> enable' command will not be displayed in 'show configuration snap-shot'. Similarly, 'loopback-test <*profile-name*> enable' is not stored in boot.cfg.
- Source MAC address is not learned on loopback port where inward loopback is enabled. Hence, port-security and dot1x authentication will not work.
- 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 address 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.
- For outward loopback test, SAP ID can be configured. SAP ID is required to fetch the mode (translate or preserve) from the input SAP ID. Since multiple SAPs can be associated with the same UNI Port, SAP ID is used to uniquely identify the SAP. If the SAP ID is not specified as an option in the outward loopback test, then SAP with the lowest SAP ID is used.
- Traffic with all the valid CVLANS, which are part of the SVLAN gets looped-back, as hardware loop-back cannot identify which CVLAN traffic to loopback.

- Consider a case with two SAPs configured, for example, SAP ID ‘X’ in translate mode and SAP ID ‘Y’ in Preserve mode. If the user configures the SAP ID Y for outward loopback, then the user must send traffic with the CVLAN that map to the configured SAP ID ‘Y’ only.
- SAP mode change must not be done when outward loopback test is running, that is, one SAP (preserve) to the other SAP (translate).

Examples

The following command examples create an ingress UNI and NNI test profile with mandatory and optional parameters:

```
-> loopback-test PE1-inward-UNI destination-mac 00:00:00:cc:aa:bb loopback-port 1/1
source-mac 00:00:00:dd:aa:01 vlan 1001 type inward

-> loopback-test PE2-inward-NNI destination-mac 00:00:00:cc:aa:bc loopback-port 2/1

-> 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
```

The following command examples create an egress UNI and NNI test profile with mandatory and optional parameters:

```
-> loopback-test PE2-outward-UNI destination-mac 00:00:00:cc:ab:bb loopback-port 1/
1 source-mac 00:00:00:dd:ab:01 vlan 1001 type outward

-> loopback-test PE1-outwardNNI destination-mac 00:00:00:dd:ab:01b loopback-port 2/
1 vlan 1001 type outward sap 6


-> 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
```

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 6450

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    Sap
-----------+------------+-------------------+-------+------+---------+----------+--------
test1          Any         00:00:00:00:00:20     Any     1/1    Inward    Config    None
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**).
Sap	The SAP ID configured.

Release History

Release 6.4.3; command was introduced.

Related Commands

loopback-test	Configures a wire-speed Ethernet loopback test profile and enables or disables the activation of the profile.

MIB Objects

N/A

29 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.MIB
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** **ethoam association allowed-cvlan-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 ccm** **ethoam endpoint priority** **ethoam endpoint lowest-defect-priority** **ethoam endpoint domain association direction** **ethoam endpoint ctag-priority**
EthOAM Loopback and Linktrace Commands	**ethoam loopback** **ethoam linktrace**
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 Monitoring Commands	**show ethoam** **show ethoam domain** **show ethoam domain association** **show ethoam domain association end-point** **show ethoam default-domain** **show ethoam default-domain configuration** **show ethoam remote-endpoint domain** **show ethoam cfmstack** **show ethoam linktrace-reply domain association endpoint tran-id** **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 6450

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 is 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 6.6.2; command introduced

Related Commands

show ethoam vlan	Displays the associations of the specified VLAN.

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-unit | 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 6450

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 6.6.1; command introduced.
Release 6.6.2; *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
   dot1agCfmMdFormat
   dot1agCfmMdLevel
```

ethoam domain mhf

Configure the Mip Half 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
mhf	**none**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Domain must be created before it is modified.

Examples

```
-> ethoam domain MD mhf default
```

Release History

Release 6.6.1; command introduced.
Release 6.6.2 *domain_name* | *mac_address* parameters replaced with *name* parameters.

Related Commands

show ethoam domain	Displays the information of a specific Management Domain 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
id-permission	**none**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Domain must be created before it is modified.

Examples

```
-> ethoam domain MD id-permission chassisid
```

Release History

Release 6.6.2; command 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 6450

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 6.6.1; command introduced.
Release 6.6.2; *association_name, domain_name | mac_address* parameters replaced with *ma-name, md-name* parameters; **unsignedint** and **icc-based** parameters added; **integer** parameter deleted.

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 6450

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 defer
```

Release History

Release 6.6.1; command introduced.
Release 6.6.2; *association_name, domain_name | mac_address* parameters replaced with *ma-name, md-name* parameters; **defer** parameter added.

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-name* **id-permission {none | chassisid | 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	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 6450

Usage Guidelines

MA must be created before it is modified.

Examples

```
-> ethoam association MA domain MD id-permission defer
```

Release History

Release 6.6.2; command 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

association_name	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
domain_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.
interval-invalid	Specifies that no CCMs are sent by a MEP
interval100ms	Specifies that 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 6450

Usage Guidelines

- The *association_name* must be unique amid all those used by or available to the service provider within a domain.
- The domain and association must be created before configuring 100ms CC interval.

Examples

```
-> ethoam association alcatel-lucent-sales domain esd.alcatel-lucent.com
ccm-interval interval10s
-> ethoam association MA domain MD ccm-interval interval100ms
```

Release History

Release 6.6.1; command introduced.
Release 6.6.3; interval100ms added.

Related Commands

show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMa
   dot1agCfmMaIndex
   dot1agCfmMaFormat
   dot1agCfmMaName
   dot1agCfmMaVid
   dot1agCfmMaMhfCreation
   dot1agCfmMaCcmInterval
   dot1agCfmMaRowStatus
```

ethoam association endpoint-list

Modifies the MEP list of an Ethernet OAM Maintenance Association.

ethoam association *association_name* **domain {***domain_name* | *mac_address***}**
endpoint-list *mep_id***[-***mep_id2***]**

no ethoam association *association_name* **domain {***domain_name* | *mac_address***}**
endpoint-list *mep_id***[-***mep_id2***]**

Syntax Definitions

association_name	Name of the Ethernet OAM Association. Up to 48 (minus domain name length) characters may be used.
domain_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.
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 6450

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 *association_name* should be unique within a domain.

Examples

```
-> ethoam association alcatel-lucent-sales domain esd.alcatel-lucent.com endpoint-
list 100-200
-> no ethoam association alcatel-lucent-sales domain esd.alcatel-lucent.com
endpoint-list 100-200
```

Release History

Release 6.6.1; command introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

```
Dot1agCfmMa
   dot1agCfmMaIndex
   dot1agCfmMaFormat
   dot1agCfmMaName
   dot1agCfmMaVid
   dot1agCfmMaMhfCreation
   dot1agCfmMaCcmInterval
   dot1agCfmMaRowStatus
Dot1agCfmMaMepList
   dot1agCfmMaMepListIdentifier
   dot1agCfmMaMepListRowStatus
```

ethoam association allowed-cvlan-list

Allows to add or delete the allowed CVLANs on the Ethernet OAM Maintenance Association (MA).

ethoam association *association_name* **domain {***domain_name* | *mac_address***}**
allowed-cvlan-list *num* **[-***num2***]**

no ethoam association *association_name* **domain {***domain_name* | *mac_address***}**
allowed-cvlan-list *num* **[-***num2***]**

Syntax Definitions

association_name	Name of the Ethernet OAM Association. Up to 48 (minus domain name length) characters can be used.
domain_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.
num	List of customer VLAN IDs allowed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use the **no** form of this command to remove the allowed CVLAN ID list.
- Note that only the CVLANs in the Ethernet Service corresponding to the SVLAN of the MA can be associated to the CVLAN list of MA.

Examples

```
-> ethoam association MA domain MD allowed-cvlan-list 10-15
-> no ethoam association MA domain MD allowed-cvlan-list 10-15
```

Release History

Release 6.6.5; command introduced.

Related Commands

show ethoam domain association	Displays the information of a specified MA in a Management Domain configured on the bridge.
ethoam endpoint	Creates a Maintenance End Point (MEP) and a virtual MEP.

MIB Objects

```
dot1agCfmMaCvlanListTable
   dot1agCfmMaCvlanListIdentifier
   dot1agCfmMaCvlanListRowStatus
```

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 6450

Usage Guidelines

N/A

Examples

```
-> clear ethoam statistics
-> clear ethoam statistics domain MD association MA endpoint 10
```

Release History

Release 6.6.2; command 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

Configures the effective value of ‘level’ for all Default Maintenance Domain (MD) entries with ‘level’ configured as ‘-1’.

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 6450

Usage Guidelines

MD Level shall range from 0 to 7.

Examples

```
-> ethoam default-domain level 1
```

Release History

Release 6.6.2; command introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.

MIB Objects

```
dot1agCfmDefaultMdDefLevel
```

ethoam default-domain mhf

Configures the effective ‘mhf’ value for all Default Maintenance Domain (MD) entries with ‘mhf’ configured as ‘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 6450

Usage Guidelines

N/A

Examples

```
-> ethoam default-domain mhf default
```

Release History

Release 6.6.2; command 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 MD entries with ‘id-permission’ configured as ‘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 6450

Usage Guidelines

N/A

Examples

```
-> ethoam default-domain id-permission chassisid
```

Release History

Release 6.6.2; command introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.

MIB Objects

```
dot1agCfmDefaultMdDefIdPermission
```

ethoam default-domain primary-vlan

Configures the level, mhf and id-permission of a Default-MD entry for a specified 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 and its value is -1. So level is determined by scalar object 'dot1agCfmDefaultMdDefLevel'
num	MD Level and it ranges from 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	The creation of MHFs is determined by the corresponding scalar object 'dot1agCfmDefaultMdDefMhfCreation'.
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 scalar object 'dot1agCfmDefaultMdDefIdPermission'.

Defaults

parameter	default
no-level | *num*	*no-level*
none | **explicit** | **default** | **defer**	**defer**
none | **chassisid** | **defer**	**defer**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

On modification of 'mhf' for any primary VID, Automip shall be 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 6.6.2; command introduced.

Related Commands

show ethoam default-domain Displays the information of all the default MD.

MIB Objects

```
dot1agCfmDefaultMdTable
   dot1agCfmDefaultMdComponentId
   dot1agCfmDefaultMdPrimaryVid
   dot1agCfmDefaultMdLevel
   dot1agCfmDefaultMdMhfCreation
   dot1agCfmDefaultMdIdPermission
```

ethoam endpoint

Creates a Maintenance End Point (MEP) and a 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* | **cvlan** *cvlan_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 the management association is created.
ma_name	Association name for the created Ethernet OAM Association.
up	The direction of the MEP is UP.
down	The direction of the MEP is DOWN.
slot/port	Physical slot and port number on which MEP needs to be created.
virtual	Creates a virtual MEP.
agg_id	Linkagg Identifier on which MEP needs to be created.
vlan_id	VLAN identifier.
cvlan_id	Customer VLAN Identifier

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The domain and association must be created before MEP can be created.
- The *mep_id* must be a unique id.
- The direction for virtual MEP must always be UP.
- For creating a virtual MEP, the value of port must be given the keyword “virtual”.
- The CVLAN must be part of the allowed CVLAN list.
- The CVLAN must be configured only for UP MEPs and on User-Network (UNI) Ports.
- The CVLAN ID must be associated to the SVLAN (MA VLAN) and the UNI port using Ethernet service configuration.
- Use the **no** form of this command to delete the MEP.

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
-> ethoam endpoint 10 domain MD association MA direction up port 1/1 cvlan 20
-> no ethoam endpoint 10 domain MD association MA
```

Release History

Release 6.6.2; command introduced.
Release 6.6.3; **virtual** parameter added.
Release 6.6.5; **cvlan** 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.
ethoam association allowed-cvlan-list	Allows to add or delete the allowed CVLANs on the Ethernet OAM Maintenance Association.

MIB Objects

```
dot1agCfmMdTable
   dot1agCfmMdName
dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepIfIndex
   dot1agCfmMepPrimaryVid
   dot1agCfmMepCvlanId
```

ethoam endpoint admin-state

Configures the administrative state of MEP.

ethoam endpoint *mep_id* **domain {***domain_name* | *mac_address***} association** *association_name* **admin-state {enable | disable}**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
domain_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.
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

N/A

Platforms Supported

OmniSwitch 6450

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-lucent-
sales admin-state enable
```

Release History

Release 6.6.1; command 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 endpoint ccm

Configures the MEP to generate Continuity Check Messages (CCM).

ethoam endpoint *mep_id* **domain {***domain_name* | *mac_address***} association** *association_name* **ccm {enable | disable}**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
domain_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.
association_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 6450

Usage Guidelines

- The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.
- Defects are logged when CCM generation is enabled and there is a loss in connectivity between two connected MEPs.

Examples

```
-> ethoam endpoint 100 domain esd.alcatel-lucent.com association
alcatel-lucent-sales ccm enable
```

Release History

Release 6.6.1; command 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 endpoint priority

Configures the priority values for CCMs and Linktrace Messages (LTMs) transmitted by a MEP.

ethoam endpoint *mep_id* **domain {***domain_name* | *mac_address***} association** *association_name* **priority** *ccm_ltm_priority*

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
domain_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.
association_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 6450

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-lucent-
sales priority 6
```

Release History

Release 6.6.1; command 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 endpoint lowest-defect-priority

Configures the lowest priority fault alarm for the lowest priority defect for a MEP.

ethoam endpoint *mep_id* **domain {***domain_name* | *mac_address***} association** *association_name* **lowest-defect-priority** *lowest_priority_defect*

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
domain_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.
association_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 6450

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-lucent-
sales lowest-defect-priority all-defect
```

Release History

Release 6.6.1; command 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 endpoint domain association direction

Creates a MEP.

ethoam endpoint *mep-id* **domain** *md-name* **association** *ma-name* **direction {up | down} {port** *slot/port* **| linkagg** *id***} [primary-vlan** *vlan-id***]**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
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.
up	For UP MEP.
down	For DOWN MEP.
slot/port	Physical slot and port number on which MEP needs to be created.
id	Linkagg Identifier on which MEP needs to be created.
vlan-id	VLAN identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 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
```

Release History

Release 6.6.2; command 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
dot1a gCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmMepDirection
   dot1agCfmMepIfIndex
   dot1agCfmMepPrimaryVid
```

ethoam endpoint ctag-priority

Configures the priority value to be included in the inner tag of the CFM frames originating from CVLAN MEPs.

ethoam endpoint *mep-id* **domain** *md-name* **association** *ma-name* **ctag-priority {copy-outer-to-inner |** *num***}**

Syntax Definitions

mep_id	Specifies the Maintenance Association End Point. The valid range is 1–8191.
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.
copy-outer-to-inner	Copies the outer tag priority to the inner tag.
num	Specify an Inner tag Priority value. Valid range is 0 to 7.

Defaults

parameter	default
copy-outer-to-inner | *num*	**copy-outer-to-inner**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

If the priority value is not specified, then the priority value of the inner tag will be the same as the priority value of the outer tag.

Examples

```
-> ethoam endpoint 1 domain md1 association ma1 ctag-priority 6
-> ethoam endpoint 1 domain md1 association ma1 ctag-priority copy-outer-to-inner
```

Release History

Release 6.6.5; command 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

```
dot1agCfmMepTable
   dot1agCfmMepCtagPriority
   dot1agCfmMepCtagSet
```

ethoam loopback

Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

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	Specifies the number of loopback messages to be transmitted. The 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	Specifies the 3-bit value to be used in the VLAN tag, if present in the transmitted frame. The 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
true | false	**true**
vlan-priority	**CCM priority**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- This command allows an operator to generate a loopback message for the specified MEP.
- This command signals the MEP that it should transmit loopback messages and detect the presence or lack of the corresponding loopback reply(s).
- Note that a loopback message is used for fault verification.
- This command also validates the connectivity between Maintenance End Points (MEP) and Maintenance Intermediate Points (MIP).

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 6.6.1; command introduced.
Release 6.6.2; *tar_mep_id,mac_address, src_mep_id, domain_name | mac_address, association_name, number_of_messages, data_size, vlan_priority* parameters replaced with *t-mepid, mac_add, s-mepid,d-name, a-name, num, string, vlan-priority*.

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 linktrace

Enables the maintenance entity to initiate transmitting Link Trace Messages (LTM).

ethoam linktrace {target-macaddress *mac_address* **| target-endpoint** *tar_mep_id***} source-endpoint** *src_mep_id* **domain {***domain_name* | *mac_address***} association** *association_name* **[flag {fdbonly | fdb-mpdb}] [hop-count** *hop_count***]**

Syntax Definitions

mac_address	Target MAC address to be transmitted.
tar_mep_id	Specifies the MEP for which the Loopback message is targeted.
src_mep_id	Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
domain_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.
association_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 is used to decide the egress port.
fdb-mpdb	Specifies that if the bridge's forwarding table could not produce a unique egress port, then the information stored in MIPCCM's database is used to determine 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 0-255.

Defaults

parameter	default
hop_count	64
flag	**fdbonly**

Platforms Supported

OmniSwitch 6450

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-endpoint 4 domain
esd.alcatel-lucent.com association alcatel-lucent_sales flag fdbonly hop-count 32
Transaction Id: 6943

-> ethoam linktrace target-endpoint 15 source-endpoint 4 domain esd.alcatel-
lucent.com association alcatel-lucent_sales
Transaction Id: 6943
```

Release History

Release 6.6.1; command introduced.
Release 6.6.2; **fdb-mpdb** parameter added.

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 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 {***domain_name* **|** *mac_address***} association** *association_name*

no ethoam fault-alarm-time endpoint *endpoint_id* **domain {***domain_name* **|** *mac_address***} association** *association_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.
mac_address	Specifies the CFM system MAC address.
domain_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
association_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 6450

Usage Guidelines

- Use the **no** form of this command to restore the Fault Notification Generation Alarm timeout value to its default value.
- The Fault Notification Generation Alarm timeout value is configurable per MEP.

Examples

```
-> ethoam fault-alarm-time 10 endpoint 100 domain esd.alcatel-lucent.com associa-
tion alcatel-lucent_sales
-> no ethoam fault-alarm-time endpoint 100 domain esd.alcatel-lucent.com associa-
tion alcatel-lucent_sales
```

Release History

Release 6.6.1; command 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 is only re-enabled if no new faults are received during this time interval.

ethoam fault-reset-time *centiseconds* **endpoint** *endpoint_id* **domain {***mac_address* | *domain_name***} association** *association_name*

no ethoam fault-reset-time endpoint *endpoint_id* **domain {***mac_address* | *domain_name***} association** *association_name*

Syntax Definitions

centiseconds	The Fault Notification Generation Reset timer 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.
mac_address	Specifies the CFM system MAC address.
domain_name	Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
association_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 6450

Usage Guidelines

- Use the **no** form of this command to restore the Fault Notification Generation Reset timeout value to its default value.
- The Fault Notification Generation Reset timer value is configurable per MEP.

Examples

```
-> ethoam fault-reset-time 10 end-point 100 domain esd.alcatel-lucent.com associa-
tion alcatel-lucent_sales
-> no ethoam fault-reset-time end-point 100 domain esd.alcatel-lucent.com associa-
tion alcatel-lucent_sales
```

Release History

Release 6.6.1; command 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. Valid 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 6450

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 associa-
tion MA vlan-priority 4

-> ethoam one-way-delay target-macaddress 00:e0:b1:6a:52:4c source-endpoint 12
domain MD association MA vlan-priority 4
```

Release History

Release 6.6.2; 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 6450

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 associa-
tion 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 6.6.2; command was introduced

Related Commands

show ethoam two-way-delay	Displays the two-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
    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

one-way-delay-table	Clears one-way delay measurement (1DM) entries.
two-way-delay-table	Clears two-way delay measurement (DMM/DMR) entries.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> clear ethoam one-way-delay-table
-> clear ethoam two-way-delay-table
```

Release History

Release 6.6.2; 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 6450

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-lucent-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 6.6.1; command introduced.

Related Commands

ethoam domain	Creates an Ethernet domain.

MIB Objects

```
Dot1agCfmStack
   dot1agCfmStackMacAddress
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.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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
      CVLAN-List (CVLAN-Id) : 1-127 301
```

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.
Primary Vlan	The Primary VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 is 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-List (MEP-Id)	Indicates the Maintenance End Point.
CVLAN-List (CVLAN-Id)	The allowed CVLAN list configured for a MEP.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; *domain_name* | *mac_address* parameters replaced with *md-name* parameter.
Release 6.6.5; CVLAN-List (CVLAN-Id) field added in the output.

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.
ethoam association allowed-cvlan-list	Allows to add or delete the allowed CVLANs on the Ethernet OAM Maintenance Association.

MIB Objects

```
Dot1agCfmMd
   dot1agCfmMdLevel
   dot1agCfmMdMhfCreation
   dot1agCfmMdTable
   dot1agCfmMdName
Dot1agCfmMa
   dot1agCfmMaName
   dot1agCfmMaVid
   dot1agCfmMaMhfCreation
   dot1agCfmMaCcmInterval
Dot1agCfmMep
   dot1agCfmMepIdentifier
   dot1agCfmMaCvlanListEntry
```

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 6450

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD association MA
Total number of MEPs configured in this MA = 2
MA-Format : string,
Primary Vlan : 200,
Associated Vlan-list : none,
Total Number of Vlans : 1,
MA-MHFstatus : mhfDefault,
MA-IdPermission : sendIdDefer,
CCM-interval : interval10s,
MEP-List(MEP-Id) : 11-30,
CVLAN-List(CVLAN-Id) : 20-30

Legend: MEP-Id: * = Inactive Endpoint


MEP-ID   Admin State Direction   Mac-Address         Port    Primary Vlan      Cvlan
--------+-----------+----------+-------------------+--------+-----------------+------------
     11      enable         up   E8:E7:32:72:01:A4   1/1       200              30
     12      enable         up   E8:E7:32:72:01:A4   1/2       200              20
```

output definitions

MA-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MA. Options include **none, explicit,** and **default**.
CCM-interval	The interval between the CCM transmissions.
MEP-List (MEP-Id)	Indicates the MEP.
Admin State	Indicates the administrative state (**enable** or **disable)** of the MEP.
Direction	The direction of the MEP.

output definitions (continued)

MAC Address	The MAC address of the MEP.
Port	The slot/port number of the bridge port to which the MEP is attached.
Primary Vlan	The Primary VLAN ID monitored by the MA. If the MA is not attached to any VLAN, 0 is displayed.
CVLAN-List (CVLAN-Id)	The CVLAN configured for the MEPs in a MA.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; *domain_name | mac_address*, *association_name* parameters replaced with *md-name*, *ma-name* parameters.
Release 6.6.5; CVLAN-List (CVLAN-Id) and Cvlan fields added in the output.

Related Commands

ethoam association	Creates an Ethernet OAM Maintenance Association in the specified domain.
ethoam endpoint	Creates a Maintenance End Point (MEP) and a virtual MEP.
ethoam association allowed-cvlan-list	Allows to add or delete the allowed CVLANs on the Ethernet OAM Maintenance Association.

MIB Objects

```
Dot1agCfmMa
   dot1agCfmMaVid
   dot1agCfmMaMhfCreation
   dot1agCfmMaCcmInterval
Dot1agCfmMaNetTable
   dot1agCfmMaNetName
dot1agCfmMdTable
   dot1agCfmMdName
Dot1agCfmMep
   dot1agCfmMepIdentifier
   dot1agCfmMepActive
   dot1agCfmMepDirection
   dot1agCfmMepIfIndex
   dot1agCfmMepMacAddress
   dot1agCfmMepCvlanId
```

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* **endpoint** *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 6450

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD association MA endpoint 10
Admin State : disable,
Direction : up,
Slot/Port: virtual,
Primary Vlan : 200,
C-vlan: 20,
MacAddress: 00:E0:B1:A0:78:A3,
Fault Notification : FNG_RESET,
CCM Enabled : disabled,
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 **(enable** or **disable**) 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.
Primary Vlan	The Primary VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 is displayed.
C-vlan	The CVLAN configured for a MEP if it's a CVLAN MEP. If the MEP is SVLAN then this field will be displayed as '-'.
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**.
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 6.6.1; command introduced.
Release 6.6.2; *domain_name | mac_address, association_name, endpoint_id* parameters replaced with *md-name, ma-name, and mep-id* parameters.
Release 6.6.5; C-vlan field added in the output.

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

```
Dot1agCfmMaNetTable
   dot1agCfmMaNetName
Dot1agCfmMdTable
   dot1agCfmMdName
Dot1agCfmMep
   dot1agCfmMepTable
   dot1agCfmMepIdentifier
   dot1agCfmMepActive
   dot1agCfmMepDirection
   dot1agCfmMepPortNumber
   dot1agCfmMepMacAddress
   dot1agCfmMepFngState
   dot1agCfmMepCcmEnabled
   dot1agCfmMepCcmLtmPriority
   dot1agCfmMepSomeRMepCcmDefect
   dot1agCfmMepErrorCcmDefect
   dot1agCfmMepXconCcmDefect
   dot1agCfmMepSomeRdiDefect
   dot1agCfmMepErrorCcmLastFailure
   dot1agCfmMepXconCcmLastFailure
   dot1agCfmMepErrMacStatus
   dot1agCfmMepLtmNextSeqNumber
   dot1agCfmMepFngAlarmTime
   dot1agCfmMepFngAlarmTime
   dot1agCfmMepLowPrDef
   dot1agCfmMepHighestPrDefect
   dot1agCfmMepCvlanId
```

show ethoam default-domain

Displays all the default MD information for all the VLANs or a specific VLAN.

show ethoam default-domain [primary-vlan *vlan_id***]**

Syntax Definitions

vlan_id	VLAN ID for which the default MD information is required. The valid range is 1–4094.

Defaults

By default, the default MD information for all VLANs is displayed.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the *vlan_id* parameter with this command to view information about the default MD for a specific VLAN.

Examples

```
-> show ethoam default-domain
Vlan   Mhf-creation   Level      Id-Permission   Status
------+-------------+---------+--------------+--------
    1           none      none      none         true
  100        default         3      none         false

-> show ethoam default-domain primary-vlan 100
Vlan   Mhf-creation   Level      Id-Permission   Status
------+-------------+---------+--------------+--------
  100        default         3      none         false
```

output definitions

Primary Vlan	The primary VLAN ID of the default MD.
Mhf-creation	Indicates the MHF value for a VLAN that is part of the default MD Options include **none**, **explicit**, or **default**.
Level	The level of the maintenance domain.
Id-Permission	The Id-Permission of the default MD for the primary VLAN ID specified or for all the VLANs. The options include none, chassisId, or defer.
Status	Indicates the status of the default MD level table entry.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; **vlan** parameter replaced with **primary-vlan**.

Related Commands

ethoam default-domain level Modifies the default Ethernet OAM Maintenance Domain (MD).

MIB Objects

```
dot1agCfmDefaultMdTable
   dot1agCfmDefaultMdComponentId
   dot1agCfmDefaultMdPrimaryVid
   dot1agCfmDefaultMdStatus
   dot1agCfmDefaultMdLevel
   dot1agCfmDefaultMdLevelVid
   dot1agCfmDefaultMdLevelLevel
   dot1agCfmDefaultMdMhfCreation
   dot1agCfmDefaultMdIdPermission
```

show ethoam default-domain configuration

Displays the values of scalar Default-MD objects.

show ethoam default-domain configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show ethoam default-domain configuration
Level : 3,
MHF-Creation : default,
ID-Permission : none
```

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**.
ID-Permission	The ID permission of the default domain. Options include none or chassisId. Configured through the **ethoam default-domain id-permission** command.

Release History

Release 6.6.2; command introduced.

Related Commands

ethoam default-domain level	Modifies the default Ethernet OAM Maintenance Domain (MD).

MIB Objects

```
dot1agCfmMaDefaultMdDefLevel
   dot1agCfmMaDefaultMdDefMhfCreation
   dot1agCfmMaDefaultMdDefIdPermission
```

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 *md_name* **association** *ma_name* **endpoint** *smep-id* **[remote-mep** *rmep-id***]**

Syntax Definitions

md_name	Specifies the domain name.
ma_name	Specifies the name of the Ethernet OAM Association.
smep-id	Specifies the MEP of a specific MA. The valid range is 1–8191.
rmep-id	The remote MEP. The valid range is 1–8191.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show ethoam remote-endpoint domain MD association MA endpoint 10
Legends: PortStatusTlv: 1 = psBlocked, 2 = psUp, 3 = psNoTlv
         InterfaceStatusTlv: 1 = ifUp, 2 = ifDown, 3 = ifUnknown
         Chassisid Subtype: 7 = Locally Assigned
RMEP-ID RMEP     OkFailed  Mac Address   P/S  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   7      DUT-1
   30  RMEP_OK  334600 00:E0:B1:6E:41:64   2   1   false   7      DUT-2
```

output definitions

RMEP-ID	Indicates the remote 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.
Port Status Tlv	Port status Tlv last received.
I/f Status Tlv	The interface status TLV last received.
RDI value	State of the RDI bit in the last received CCM.

output definitions (continued)

Ch-id Subtype	Indicates the format of chassis id received in last CCM.
Ch-id	Indicates the chassis id.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; *domain_name | mac_address, association_name, endpoint_id, remote_mepid* parameters replaced with *d_name, a_name, s-mepid, r-mepid*.

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 that determines the relationship 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 is displayed.
agg_num	The aggregate ID for which the contents of the configured MEP or MIP must be displayed.
virtual	Displays the information for virtual UP MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show ethoam cfmstack port 1/3
Up MHF Configured:
  Vlan-id: 100,
  C-vlan: 20,
  Direction: up,
  MAC-Address: 00:D0:95:EC:84:B0,
  Maintenance Association: alcatel-lucent-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-lucent-sales,
  Maintenance Domain: esd.alcatel-lucent.com,
  MD-level: 3

-> show ethoam cfmstack port virtual
MEP-Id 32 - Vlan 30:
  C-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.
C-vlan	The CVLAN configured for a MEP if it's a CVLAN MEP. If the MEP is SVLAN then this field will be displayed as '-'.
Direction	Indicates the direction (**Inward** or **Outward)** of the Maintenance Point (MP) on the Bridge port.
MAC-Address	For UP MEP, the MAC-Address displayed is the System MAC adderss.For Down MEP, the MAC-Address displayed is of the port on which MEP ID is configured.
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 6.6.1; command introduced.
Release 6.6.3; **virtual** parameter introduced.
Release 6.6.5; C-vlan field added in the output displayed for **port** information.

Related Commands

ethoam endpoint	Creates an Ethernet OAM MEP in the specified MA.

MIB Objects

```
Dot1agCfmMd
   dot1agCfmMdName
Dot1agCfmMa
   dot1agCfmMaName
Dot1agCfmStack
   dot1agCfmStackVlanIdOrNone
   dot1agCfmStackDirection
   dot1agCfmStackMacAddress
   dot1agCfmStackMdLevel
   dot1agCfmMepCvlanId
```

show ethoam linktrace-reply domain association endpoint tran-id

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 6450

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 appears 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
Ttl : 63,
  LTM Forwarded : no,
  Terminal MEP : yes,
  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_HIT,
  Chassis ID Subtype : LOCALLY_ASSIGNED,
  Chassis ID : DUT-1,
```

```
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_NONE,
Egress Mac : 00:00:00:00:00:00,
Egress Port ID Subtype : 0,
Egress Port ID : not-specified
```

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**.
Chassis ID Subtype	Indicates the format of chassis id received in last CCM.
Chassis ID	Indicates the chassis id.
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.
Ingress Port ID Subtype	Indicates the format of the ingress port ID.
Ingress Port ID	Ingress port.
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.
Egress Port ID Subtype	Indicates the format of the egress port ID.
Egress Port ID	Egress port.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; *domain_name | mac_address*, *association_name*, *mep_id*, *transaction_id* parameters replaced with *d-name*, *a-name*, *s-mepid* and *num*.

Related Commands

ethoam linktrace	Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

```
dot1agCfmLtrTable
   dot1agCfmLtrTtl
   dot1agCfmLtrForwarded
   dot1agCfmLtrTerminalMep
   dot1agCfmLtrLastEgressIdentifier
   dot1agCfmLtrNextEgressIdentifier
   dot1agCfmLtrRelay
   dot1agCfmLtrChassisIdSubtype
   dot1agCfmLtrChassisId
   dot1agCfmLtrIngress
   dot1agCfmLtrIngressMac
   dot1agCfmLtrIngressPortIdSubtype
   dot1agCfmLtrIngressPortId
   dot1agCfmLtrEgress
   dot1agCfmLtrEgressMac
   dot1agCfmLtrEgressPortIdSubtype
   dot1agCfmLtrEgressPortId
```

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 6450

Usage Guidelines

N/A

Examples

```
-> show ethoam linktrace-tran-id domain esd.alcatel-lucent.com association alcatel-
lucent-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 6.6.1; command 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 associations of the specified VLAN.

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 6450

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 6.6.2; command introduced.

Related Commands

ethoam endpoint domain association direction	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 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 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 6450

Usage Guidelines

N/A

Examples

```
-> show ethoam statistics domain esd.alcatel-lucent.com association alcatel-lucent-
sales

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 esd.alcatel-lucent.com

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 esd.alcatel-lucent.com association alcatel-lucent-
sales 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.
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 6.6.1; command introduced.

Related Commands

ethoam endpoint domain association direction	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 vid**] [{port** slot/port **| linkagg** aggid**}]**

Syntax Definitions

vid	VLAN Identifier.
slot/port	Physical slot and port.
aggid	Logical Linkagg Identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show ethoam config-error
Vlan    Port   Error-type
------+------+------------
10       1/2    CFMleak
10       1/10   CFMleak
30       1/2    CFMleak

-> show ethoam config-error vlan 10
vlan    port   error-type
------+------+------------
10       1/2    CFMleak
10       1/10   CFMleak

-> show ethoam config-error port 1/2
vlan    port   error-type
------+------+------------
10       1/2    CFMleak
30       1/2    CFMleak

-> 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 6.6.2; command 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.
association	Association name for the created Ethernet OAM Association.
s-mepid	Source MEP-ID. Valid Range 1-8191.
mac-add	MAC-Address of the remote MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 happens 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

```
-> 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

-> 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.
Jitter	Type of an error.

Release History

Release 6.6.2; command 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.
association	Association name for the created Ethernet OAM Association.
s-mepid	Source MEP-ID. Valid Range 1-8191.
mac-add	MAC-Address of the remote MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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, that is, if only one reply for DMM (DMR) is received and this was the first time DMM was initiated from the MEP, then jitter is not 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

```
-> 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
```

```
-> 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

-> 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        -

-> 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 6.6.2; command 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
```

30 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 ethoam-loopback** **saa type ethoam-two-way-delay** **saa start** **saa stop** **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**

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 (for example “SAA 10”).
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 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 6450

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 exists, the CLI will return an error message, as duplicate entries are not allowed.
- Any number of SAAs can be configured (MAX 127). It is recommended not to start many aggressive SAAs (having session interval <= 10). To achieve proper scheduling of all the started SAA (aggressive and relaxed) it is recommended not to start more than 50 SAAs.

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 6.6.2; 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 (for example “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 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 24–1472 bytes.

Defaults

parameter	default
count	5
delay	1000 ms
size	24 bytes

Platforms Supported

OmniSwitch 6450

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.

- 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 1 sec. 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 6.6.2; 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 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 36–1500 bytes.

Defaults

parameter	default
vlan-priority	0
drop-eligible	false
count	5
delay	1000 ms
size	36 bytes

Platforms Supported

OmniSwitch 6450

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.
- The timeout for each ping request packet is 1 sec. This value is not configurable.
- 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 + 36] 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 6.6.2; 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 type ethoam-loopback

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 (for example “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 100 ms - 1000 ms in multiples of 100 ms.
num	The number of packets to be sent during loopback. Valid range is 1 - 100.

Defaults

parameter	default
drop-eligible true | false	false
num-pkts	5
delay	1000

Platforms Supported

OmniSwitch 6450

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 **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 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 6.6.2; 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 ETH-DMM, including the number of packets and inter-packet delay parameters.

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 (for example “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 100 ms - 1000 ms in multiples of 100 ms.
num	The number of packets to be sent during loopback. Valid range is 1–100.

Defaults

parameter	default
num	5
delay	1000

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The SAA should exist before issuing the CLI. If the SAA does not exist, the CLI will return error.
- The source MEP-ID, MD, and MA must be created before initiating DMM.
- If the source MEP-Id/MA/MD does not exist, the configuration will be accepted and no error will be returned.
- When the **target-endpoint** parameter is specified, then it must be learned before initiating DMM.
- When the **target-endpoint** parameter is specified and learned, ETH-DMM will be transmitted irrespective of whether the RMEP state is OK or failed.

- 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 **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.
- 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 1 sec. 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 6.6.2; 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 start

Starts the SAA test.

saa *string* **start [at** *yyyy-mm-dd,hh:mm:ss.ds***]**

Syntax Definitions

string	An existing SAA ID string.
yyyy-mm-dd,hh:mm:ss.ds	The date and time to start the SAA.

Defaults

By default, the SAA test is started immediately.

Platforms Supported

OmniSwitch 6450

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 error.
- If the SAA type is configured with a source IP that does not exist or is not active, then the packet will not be transmitted and no error will be returned. Swlogs will be updated.
- ICMP must be enabled on the switch. If ICMP is disabled and an SAA of type ‘ip-ping’ 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 SAA type is configured with a source MEP that does not exist or is not active (admin down), then the packet will not be transmitted and no error will be returned on the CLI console. Swlogs will be updated.
- It is recommended that all the SAAs be rescheduled if the system time is being changed.

Examples

```
-> saa saa2 start at 2009-09-12,09:00:00
-> saa saa4 start
```

Release History

Release 6.6.2; 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 6450

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 6.6.2; command was introduced.

Related Commands

show saa	Displays SAA configuration information.
show saa statistics	Displays SAA statistics.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlStopAt
```

saa jitter-calculation

Calculates jitter values on each SAA probe. Each and every jitter that is calculated will be implemented as per the formula specified in RFC 1889.

saa jitter-calculation {default|enhanced}

Syntax Definitions

default	Specifies that the jitter value will be calculated as per old design.
enhanced	Specifies that the jitter calculation will be made as per RFC defined formula.

Defaults

By default, the mode will be set to **default** which will calculate the jitter value as per old design.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- By default the mode will be sent to **default** which will calculate the jitter value as per old design.
- As per the old design the inter-arrival jitter calculation is based on the Round Trip Time difference between two successive packets.
- When the jitter calculation mode is set to **enhanced** then jitter calculation will be made as per RFC defined formula.
- The new implementation is to calculate inter-arrival jitter based on the below formula specified in RFC 1889.
- Formula: Jitter = Jitter + (abs (ElapsedTime - OldElapsedTime) - Jitter) / 16

  Where
  'Jitter' - Jitter value calculated from successive packets RTT.
  Elapsed - RTT value involved in the packet.

Examples

```
-> saa jitter-calculation default
-> saa jitter-calculation enhanced
```

Release History

Release 6.7.2; command was introduced.

Related Commands

show saa	Displays the mode which is set for jitter calculation.

MIB Objects

```
alaSaaJitterCalcModeConfig
alaSaaCtrlJitterCalculationMode
```

show saa config

Displays the mode which is set for jitter calculation.

show saa config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show saa config
   Jitter-calculation:enhanced
```

Release History

Release 6.7.2; command was introduced.

Related Commands

saa jitter-calculation	Calculates jitter values on each SAA probe. Each and every jitter that is calculated will be implemented as per the formula specified in RFC 1889.

MIB Objects

```
alaSaaJitterCalcModeConfig
alaSaaCtrlJitterCalculationMode
```

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 6450

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 started200          2010-01-16,15:20:05.0  success     Two way test
```

Release History

Release 6.6.2; 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 {mac-ping | ip-ping | ethoam-loopback | ethoam-two-way-delay} config**

Syntax Definitions

string	An existing SAA ID string.
mac-ping	Displays MAC Ping SAAs
ip-ping	Displays IP Ping SAAs.
ethoam-loopback	Displays ETH-LB SAAs.
ethoam-two-way-delay	Displays ETH-DMM SAAs.

Defaults

By default, all SAAs with the specified type are displayed.

Platforms Supported

OmniSwitch 6450

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

-> 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
```

Release History

Release 6.6.2; command was introduced.

Related Commands

saa type mac-ping	Configures a MAC ping SAA.
saa type ip-ping	Configures an IP ping SAA.
saa type ethoam-loopback	Configures an ETH-LB SAA.
saa type ethoam-two-way-delay	Configures an ETH-DMM SAA.

MIB Objects

```
alaSaaCtrlTable
   alaSaaCtrlTestIndex
   alaSaaCtrlDescr
   alaSaaCtrlInterval
   alaSaaCtrlTestMode
alaSaaMacCtrlTable
   alaSaaMacCtrlDstAddress
   alaSaaMacCtrlPayloadSize
   alaSaaMacCtrlInterPktDelay
   alaSaaMacCtrlNumPkts
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 6450

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 of each SAA test and in each SAA history, iteration information of first 20 received packets are stored.
- Use the *string* parameter to display statistics for a specific SAA.
- Statistics and history do not persist across a switch reboot or takeover.
- An aggregated record is maintained for each SAA. This record maintains aggregated information of all the iterations that are run and is updated after every iteration. After Nth iteration, the record is updated as shown below:

RTT Min	Minimum (delayOfIteration1,delayOfIteration2,....., delayOfIterationN)
RTT Avg	[(avgDelayIteration1 * pktsRcvdInIteration1)+(avgDelayIteration2 *pktsRcvdInIteration2)+ . . . +(avgDelayIterationN * pktsRcvdInIterationN)] / (pktsRcvdInIteration1 + pktsRcvdInIteration2 + . . . + pktsRcvdInIterationN)
RTT Max	(delayOfIteration1, delayOfIteration2,....., delayOfIterationN)
Jitter Min	Minimum (jitterOfIteration1, jitterOfIteration2,...., jitterOfIterationN)
Jitter Avg	[(avgJitterIteration1 * {pktsRcvdInIteration1 - 1}) + (avgJitterIteration2 * {pktsRcvdInIteration2 - 1})+ . . . + (avgJitterIterationN * {pktsRcvdInIterationN-1})] / ({pktsRcvdInIteration1-1}+{pktsRcvdInIteration2-1}+ . . . + {pktsRcvdInIterationN-1})
Jitter Max	Maximum (jitterOfIteration1, jitterOfIteration2,...., jitterOfIterationN)

When a new iteration is run, the record is updated as shown below:

RTT Min	Minimum (previousDelay, latestIterationDelay)
RTT Avg	[(aggregatedDelay * totalNumPktsRcvd) + (latestIterationDelay * latestNumPktsRcvd)] / (totalNumPktsRcvd + latestNumPktsRcvd)
RTT Max	Maximum (previousDelay, latestIterationDelay)
Jitter Min	Minimum (previousJitter, latestIterationJitter)
Jitter Avg	{aggregatedJitter * (totalJitterSamplesRcvd)} + {latestIterationJitter * (latestNumPktsRcvd - 1)}] / {(totalJitterSamplesRcvd) + (latestPkts-Rcvd - 1)} **Note**: totalJitterSamplesRcvd represents total number of jitter samples received. A jitter sample is obtained when at least two replies are received. E.g. 5 replies received will provide 4 jitter samples in an iteration.
Jitter Max	Maximum (previousJitter, latestIterationJitter).

For failed iterations, i.e. iterations in which no reply is received, both the delay and jitter statistics are not updated. For iterations in which only one reply is received, only the delay statistics are updated and jitter statistics are not. For iterations in which more than one reply are received, for example, if 'n' replies are received, then 'n' delays and 'n-1' jitter values are calculated and used for statistics updation.

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
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
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

-> 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

-> show saa saa1 statistics aggregate
SAA: saa1
  Total numbers of iterations          : 5
  Aggregated Record:
    Total Packets Sent                 : 33,
    Total Packets Received             : 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 Received           : 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 Received             : 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 6.6.2; 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
```

31 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 administrators 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 threshold 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 6450

Usage Guidelines

N/A

Examples

```
-> efm-oam multiple-pdu-count 5
```

Release History

Release 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 threshold 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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
```

32 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 6450, 6350

Usage Guidelines

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

Examples

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

Release History

Release 6.6.1; 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 (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).
enable	Enables UDLD status on a port.
disable	Disables UDLD status on a port.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The UDLD protocol must be enabled before using this command.

Examples

```
-> udld port 1/3 enable
-> udld port 1/6-10 enable
-> udld port 2/4 disable
```

Release History

Release 6.6.1; 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 (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).
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 6450, 6350

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 of operation gets the link-up asynchonously, 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 6.6.1; 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 (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).
seconds	The probe-message transmission interval, in seconds (7-90).

Defaults

parameter	default
seconds	15

Platforms Supported

OmniSwitch 6450, 6350

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 12-18 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 6.6.1; 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 (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).
seconds	The echo based detection period, in seconds (4-15).

Defaults

parameter	default
seconds	8

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 (e.g., 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 (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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 (e.g., 3/1 specifies port 1 on slot 3).

Defaults

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

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 (e.g., 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 (e.g., 3/1 specifies port 1 on slot 3).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 (e.g., 3/1 specifies port 1 on slot 3).

Defaults

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

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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
```

33 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 through 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 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 *session_id* **[no] [user-port {slot** *slot* **|** *slot/port***[-***port2***] | linkagg** *agg_num***}] [network-port {slot** *slot* **|** *slot/port***[-***port2***] | linkagg** *agg_num***}]**

Syntax Definitions

session_id	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 6450, 6350

Usage Guidelines

- User ports that are part of one session cannot communicate with each other and can communicate only through 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 6.6.3; 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 session.

MIB Objects

```
PortMappingSessionTable
   pmapSessionNumber
portMappingTable
   pmapPortIfindex
   pmapPortType
```

port mapping

Enables, disables, or deletes a port mapping session.

port mapping *session_id* **{enable | disable}**

no port mapping *session_id*

Syntax Definitions

session_id	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 6450, 6350

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 6.6.3; 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	Configures the direction of a port mapping session.
port mapping dynamic-proxy-arp	Displays the status of one or more port mapping session.
show port mapping	Displays the configuration of one or more port mapping session.

MIB Objects

```
PortMappingSessionTable
   pmapSessionNumber
   pmapSessionStatus
```

port mapping

Configures the direction of a port mapping session.

port mapping *session_id* **{unidirectional | bidirectional}**

Syntax Definitions

session_id	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 6450, 6350

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 6.6.3; 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 session.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
   PmapSessionDirection
```

port mapping dynamic-proxy-arp

Enables or disables the dynamic proxy arp functionality for the port mapping session.

port mapping *port_mapping_session id* **dynamic-proxy-arp {enable | disable}**

Syntax Definitions

port_mapping_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 6450, 6350

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 dynamic 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 configuration of the MAC Forced Forwarding feature.

Examples

```
-> portmapping 1 dynamic-proxy-arp enable
-> portmapping 1 dynamic-proxy-arp disable
```

Release History

Release 6.6.3; 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 session.
show port mapping status	Displays the status of one or more port mapping session.

MIB Objects

```
portMappingSessionTable
   pmapSessionDynProxyARP
```

show port mapping status

Displays the status of one or more port mapping session.

show port mapping [*session_id***] status**

Syntax definitions

session_id	The port mapping session ID. Valid range is 1 to 8.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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          DPA Status
------------+----------------+---------------+--------------
    8            bi             disable        disable
```

output definitions

SessionID	Displays the port mapping session ID.
Direction	Displays the direction of a port mapping session.
Status	Displays status of a port mapping session.
DPA Status	Displays the status of Dynamic proxy ARP on the port mapping session.

Release History

Release 6.6.3; 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.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
   PmapSessionDirection
   pmapSessionStatus
```

show port mapping

Displays the configuration of one or more port mapping session.

show port mapping [*session_id***]**

Syntax Definitions

session_id	The port mapping session ID. Valid range is 1 to 8.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.3; 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.

MIB Objects

```
PortMappingSessionTable
   PmapSessionNumber
   portMappingTable
   pmapPortIfindex
   pmapPortType
```

34 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 some 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. The ping command is used to determine whether network hosts are online.
- Transmission Control Protocol (TCP)—A major data transport mechanism that provides reliable, connection-oriented, full-duplex data streams. While the role of TCP is to add reliability to IP, TCP relies upon IP to do the actual delivering of datagrams.
- User Datagram Protocol (UDP)—A secondary transport-layer protocol that uses IP for delivery. UDP is not connection-oriented and does not provide reliable end-to-end delivery of datagrams. But some applications can safely use UDP to send datagrams that do not require the extra overhead added by TCP.
- The Two-Way Active Measurement Protocol (TWAMP)—An open protocol for measurement of two-way metrics. TWAMP provides a standard technique to measure network performance metrics. Unlike ICMP Ping, TWAMP also measures round trip delay/Jitter apart from the RTT.

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.
Data packets can be forwarded using IP when 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 the Routing Information Protocol (RIP). See Chapter 34, “IP Commands,” for the appropriate CLI commands. For more information on VLANs and RIP, see the applicable chapters in the *OmniSwitch AOS Release 6 Network 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 interface cvlan** **ip managed-interface** **ip interface dhcp-client** **ip router primary-address** **ip router router-id** **ip static-route** **ip route-pref** **ip default-ttl** **ping** **traceroute** **ip directed-broadcast** **ip directed-broadcast allow** **ip directed-broadcast clear** **ip service** **ip tables** **show ip traffic** **show ip interface** **show ip interface cvlan** **show ip managed-interface** **show ip route** **show ip route-pref** **show ip redist** **show ip access-list** **show ip route-map** **show ip router database** **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 set metric** **ip route-map set tag** **ip route-map set ip-nexthop** **ip route-map set ipv6-nexthop** **show ip redist** **show ip access-list** **show ip route-map**

ARP	**arp** **clear arp-cache** **ip dos arp-poison restricted-address** **arp filter** **clear arp filter** **ip arp-limit default** **ip arp-limit extend** **show arp** **show ip dynamic-proxy-arp** **show arp filter** **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**
TWAMP	**twamp server** **show twamp server info** **show twamp server connections**
TCP	**show tcp statistics** **show tcp ports**
UDP	**show udp statistics** **show udp ports**
Denial of Service (DoS)	**ip dos scan close-port-penalty** **ip dos scan tcp open-port-penalty** **ip dos scan udp open-port-penalty** **ip dos scan threshold** **ip dos trap** **ip dos scan decay** **show ip dos config** **show ip dos statistics**

ip interface

Configures an IP interface to enable IP routing on a VLAN. Without an IP interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

ip interface *name* **[address** *ip_address***] [mask** *subnet_mask***] [admin [enable | disable]] [vlan** *vid***] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [eth2 | snap] [primary | no primary] local-host-dbcast [enable | disable]**

no ip interface *name*

Syntax Definitions

name	Text string up to 20 characters. Use quotes around string if description contains multiple words with spaces between them (for example "Alcatel Marketing"). **Note:** 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.
enable	Enables the administrative status for the IP interface.
disable	Disables the administrative status for the IP interface.
vid	An existing VLAN ID number. The valid range is 1 to 4094.
forward	Enables forwarding of IP frames to other subnets.
no forward	Disables forwarding of IP frames. The router interface still receives frames from other hosts on the same subnet.
local-proxy-arp	Enables Local Proxy ARP on the specified interface.
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
enable | disable	**enable**
vid	none (unbound)
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 6450, 6350

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.

Note:
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 enabled with Local Proxy ARP is moved to another VLAN, Local Proxy ARP is enabled for the new VLAN and must be enabled on another interface for the old VLAN.

- When Local Proxy ARP is enabled, all traffic is routed instead of bridged within the VLAN. ARP requests return the MAC address of the IP router interface. Note that the same MAC address is assigned to each interface configured for a VLAN.
- Local Proxy ARP takes precedence over any switch-wide ARP or Proxy ARP function. It is not necessary to have Proxy ARP configured in order to use Local Proxy ARP. The two features are independent of each other.
- 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 always remains operationally active.

Examples

```
-> ip interface “Marketing”
-> ip interface “Payroll address” address 18.12.6.3 mask 255.255.255.0 vlan 255
-> ip interface “Human Resources” address 10.200.12.101 vlan 500 no forward snap
-> ip interface “Distr” address 11.255.14.102/24 vlan 500 local-proxy-arp primary
```

Release History

Release 6.6.1; command introduced.
Release 6.6.4; **local-host-dbcast** parameter added.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   alaIpInterfaceIpForward
   alaIpInterfaceEncap
   alaIpInterfaceLocalProxyArp
   alaIpInterfacePrimCfg
   alaIpInterfaceOperState
   alaIpInterfaceOperReason
   alaIpInterfaceRouterMac
   alaIpInterfaceBcastAddr
   alaIpInterfacePrimAct
```

Ip interface cvlan

Configures the SVLAN interface using which the SVLAN can be mapped to the CVLAN.

ip interface *name* **[address** *ipv4_address***] [mask** *subnet_mask***] cvlan** *cvlan_id* **vlan** *vlan_id*

no ip interface *name*

Syntax Definitions

name	Text string up to 20 characters. Use quotes around string if description contains multiple words with spaces between them (for example “Alcatel Marketing”). **Note:** 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.
cvlan_id	Specify the CVLAN that needs to be added inside the single tagged frames, which needs to be sent using that mapped interface.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- There is no dependency for this command upon untagged-cvlan insertion. It can be configured even when CVLAN on untagged feature is disabled.
- For a specific UNI, only one CVLAN can be mapped when CVLAN on untagged feature is enabled.

Examples

```
-> ip interface "vlan10" address 10.10.10.1 mask 255.255.255.0 cvlan 10 vlan 1001
```

Release History

Release 6.6.5; command introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceCVlanID
```

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 6450, 6350

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 it default behavior of choosing the source IP address.
- Use **all** in this command to configure a common source IP address to the applications that use the default source IP address.

Examples

```
-> ip managed-interface loopback0 application ntp
-> no ip managed-interface loopback0 application ntp
```

Release History

Release 6.6.2; command introduced.

Related Commands

show ip route	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* **ifindex** *id***] [vsi-accept-filter** *filter-string* | **server-preference] [fire-wall-vlan** *vid***][release | renew] [option-60** *opt60_string***] [admin {enable | disable}]**

no ip interface dhcp-client

ip interface dhcp-client no server-preference

Syntax Definitions

dhcp-client	Reserved IP interface name, indicates the interface must use DHCP to obtain an IP address from a DHCP server.
vid	An existing VLAN ID number. The valid range is 1 to 4094. The DHCP client will be created on this VLAN.
id	ifindex ID for the configured VLAN.
filter-string	String that matches with option-43 filed of the DHCPACK to prefer the desired OXO server. By default the filter-string will be empty string (“ “).
server-preference	Enables DHCP server precedence logic. The DHCP server preference logic is mutually exclusive with vsi-accept-filter.
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 or request packets.
enable	Enables the administrative status for the IP interface.
disable	Disables the administrative status for the IP interface.
firewall-vlan	Designates a VLAN to be a firewall VLAN.

Defaults

parameter	default
opt60_string	The switch model (eg. 6350-P10).
enable | disable	enable
filter-string	“ “
server-preference	disabled

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove the dhcp-client IP interface.
- If the system name is not configured, it is updated using the option-12 field.
- If the length of option-12 string is greater than 19 characters the remaining characters are truncated.
- The minimum lease time accepted on the dhcp-client interface is five minutes.
- The VSI filter-string once configured cannot be deleted. It can be overwritten or modified. It can be configured as empty string (“ “).
- The VSI accept filter is case-sensitive. The maximum length of a vsi-accept-filter can be of 64 character length.
- In order to retain the same OXO server which was configured before RCL, the VSI filter must match the hard coded string “alcatel.a4400.0”.
- To create an IP interface for firewall VLAN, use the **firewall-vlan** keyword, followed by the VLAN ID.
- DHCP client preference to obtain the lease from the highest priority server among the multiple offers received can be enabled using the **server-preference** option.
- Server preference option can also be set without specifying VLAN ID, provided the dhcp-client interface is associated with a VLAN prior to setting the server preference.
- The **server-preference** option is mutually exclusive with **vsi-accept-filter** option.
- Use the **no server-preference** option to remove the server preference.
- The server preference details can be viewed using the **show ip interface dhcp-client** command.

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
-> ip interface dhcp-client vlan 1 ifindex 1
-> ip interface dhcp-client vsi-accept-filter “alcatel.a4400.0”
-> ip interface firewall address 11.1.1.1 firewall-vlan 173
-> ip interface dhcp-client vlan 1 server-preference
-> ip interface dhcp-client server-preference
-> ip interface dhcp-client no server-preference
```

Release History

Release 6.6.2; command introduced.
Release 6.6.4; **vsi-accept-filter** parameters included.
Release 6.7.2.R04; **server-preference** parameters included.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceDhcpStatus
   alaIpInterfaceDhcpIpRelease
   alaIpInterfaceDhcpIpRenew
   alaIpInterfaceDhcpVsiAcceptFilterString
   alaIpInterfaceDhcpOption60String
   alaIpInterfaceFirewallVlanID
   alaIpInterfaceDhcpServerPreference
   alaIpInterfaceVlanID
```

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 6450, 6350

Usage Guidelines

- The router primary address must 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 6.6.1; 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 6450, 6350

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.

Examples

```
-> ip router router-id 172.22.2.115
```

Release History

Release 6.6.1; command introduced.

Related Commands

ip router primary-address	Configures the router primary IP address.

MIB Objects

```
alaDcrTmConfig
   alaDrcTmIpRouterId
```

ip static-route

Creates or deletes an IP static route. Static routes are user-defined; they carry a higher priority than routes created by dynamic routing protocols. That is, static routes always have priority over dynamic routes, regardless of the metric value.

ip static-route *ip_address* **[mask** *mask***] gateway** *gateway* **[metric** *metric***]**

no ip static-route *ip_address* **[mask** *mask***] gateway** *ip_address* **[metric** *metric***]**

Syntax Definitions

ip_address	Destination IP address of the static route.
mask	Subnet mask corresponding to the destination IP address.
gateway *ip_address*	IP address of the next hop used to reach the destination IP 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 1–15.

Defaults

parameter	default
metric	1

Platforms Supported

OmniSwitch 6450, 6350

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.
- 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.
- Multiple static routes can be added to a subnet of directly connected network. Use **show ip route** command to view the static routes added.

Examples

```
-> ip static-route 171.11.0.0 gateway 171.11.2.1
-> ip static-route 0.0.0.0 mask 0.0.0.0 gateway 171.11.2.1
```

Release History

Release 6.6.1; command introduced.

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
   alaIprmStaticRouteStatus
```

ip route-pref

Configures the route preference of a router.

ip route-pref {static | rip | ebgp | ibgp} *value*

Syntax Definitions

static	Configures the route preference of static 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.
value	Route preference value.

Defaults

parameter	default
static *value*	2
rip *value*	120
ebgp *value*	190
ibgp *value*	200

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Route preference of local routes cannot be changed.

Examples

```
-> ip route-pref ebgp 20
-> ip route-pref rip 60
```

Release History

Release 6.6.3; command introduced.

Related Commands

show ip route-pref	Displays the configured route-preference of a router.

MIB Objects

```
alaIprmRtPrefTable
   alaIprmRtPrefLocal
   alaIprmRtPrefStatic
   alaIprmRtPrefRip
   alaIprmRtPrefEbgp
   alaIprmRtPrefIbgp
```

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 can 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 6450, 6350

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 6.6.3; 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** *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 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 4–60000.
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
count	6

parameter	default
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 6450, 6350

Usage Guidelines

- Modifying the default values for the ping command is applied only for the current ping. When command is used again for the next time, the default values are used unless modified with 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.
- If the Don't Fragment (DF) bit is set, and the IP packet is larger than the MTU, the IP packet is dropped.
- The Ping command does not support Loose, Strict, and route record options.

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 6.6.3; command introduced.

Related Commands

traceroute	Finds the path taken by an IP packet from the local switch to a specified destination.

MIB Object

N/A

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 at which point the 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 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 6450, 6350

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 Loop-back0 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.

Examples

```
-> traceroute 135.254.170.199 max-hop 5 min-hop 1 port-number 1025
source-interface Loopback0 timeout 5

traceroute to 135.254.170.199, 5 hops max, 40 byte packets
 1  10.135.33.1  2 ms  2 ms  11 ms
 2  135.250.9.97  6 ms  6 ms  4 ms
 3  135.250.9.153  4 ms  4 ms  3 ms
 4  135.254.170.199  3 ms  3 ms  3 ms
```

Release History

Release 6.6.3; command introduced.

Related Commands

show ip route	Displays the IP Forwarding table.

MIB Object

N/A

ip directed-broadcast

Enables or disables IP directed broadcasts routed through the switch. An IP directed broadcast is an IP datagram that has all 0 or all 1 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 | controlled}

Syntax Definitions

on	Enables IP directed broadcasts.
off	Disables IP directed broadcasts.
controlled	Broadcasts only the IP packets received from the user defined source.

Defaults

The default value is **off**.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Directed broadcasts are used in denial-of-service “smurf” attacks. A continuous stream of ping requests are sent from a falsified source address to a directed broadcast address in a smurf attack. This stream of requests result in a large stream of replies, which can overload the host of the source address. By default, the switch drops directed broadcasts. Typically, directed broadcasts must not be enabled.
- If the **controlled** mode is set, then the user needs to mention the trusted information such as source IP address, destination IP address, and VLAN information to broadcast the packet. If the information is not specified, then the broadcast packets will not be processed.

Examples

```
-> ip directed-broadcast off
-> ip directed-broadcast controlled
```

Release History

Release 6.6.3; command introduced.
Release 6.7.2.R02; **controlled** keyword added.

Related Commands

ip directed-broadcast allow	Specify the source IP address, destination IP address, and VLAN information to broadcast the packets in controlled manner.
show ip interface	Displays the status and configuration of IP interfaces.
show ip route	Displays the IP Forwarding table.
show ip config	Displays IP configuration parameters.

MIB Objects

```
alaIpDirectedBroadcast
```

ip directed-broadcast allow

Specify the source IP address, destination IP address, and VLAN information to broadcast the packets in controlled manner. The specified information is considered as the trusted information to broadcast the packets received only from the defined source, and the remaining broadcast packets are dropped.

ip directed-broadcast allow source-ip *ip_address* **[mask** *subnet_mask***] [destination-ip** *ip_address* **[mask** *subnet_mask***] | vlan** *vlan_id***]**

no ip directed-broadcast source-ip *ip_address*

Syntax Definitions

source-ip *ip_address*	Source IP address from which the broadcast packets are received.
destination-ip *ip_address*	Destination address to which the packets must be directed.
subnet_mask	A valid IP address mask.
vlan_id	Existing VLAN ID to which the packets are to be directed.

Defaults

parameter	default
ip_address	0.0.0.0
subnet_mask	IP address class/0.0.0.0
vlan_id	None

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** command to remove the trusted information configured with the source IP address for controlled IP directed-broadcast.
- If the source IP matches, then the packets are broadcasted in the particular destination IP interface or VLAN interfaces. The remaining packets are dropped.
- When the packet received matches with the source IP and if the destination and VLAN information are not defined by the user, then the packet will be forwarded based on the routing information in the switch.
- If the destination IP or VLAN is defined by the user, then the destination address of the packet will be matched with the user defined list and routes the packets if the destination IP matches, else the packet are dropped. If the VLAN information is defined, then the packets will be routed through the interface configured in the VLAN.
- If the destination IP is not reachable or if the destination subnet is not directly connected, packet will be dropped

- If the directed-broadcast is set to controlled mode and the user does not specify any trusted information, all the broadcast packets will be dropped. This case is equivalent to disabled state of directed-broadcast.
- 32 source IP addresses can be defined, and each source IP address can have 30 destination IP address and VLAN information.

Examples

```
-> ip directed-broadcast allow source-ip 30.0.0.10/24
-> ip directed-broadcast allow source-ip 30.0.0.10/24 destination-ip 10.0.0.255/24
-> ip directed-broadcast allow source-ip 30.0.0.10/24 vlan 10
-> ip directed-broadcast allow source-ip 30.0.0.10/24 destination-ip 10.0.0.255/24
vlan 10
-> ip directed-broadcast allow source-ip 30.0.0.10 mask 255.255.255.0
-> ip directed-broadcast allow source-ip 30.0.0.10 mask 255.255.255.0 destination-
ip 10.0.0.255 mask 255.255.255.0

-> no ip directed-broadcast source-ip 30.0.0.10
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

ip directed-broadcast	Enables or disables IP directed broadcasts routed through the switch.
ip directed-broadcast clear	Clears all the trusted information configured.
show ip config	Displays IP configuration parameters.

MIB Objects

```
alaIpDirectedBroadcast
alaIpDirectedBroadcastCtrlSrcAddr
alaIpDirectedBroadcastCtrlSrcMask
alaIpDirectedBroadcastCtrlDstAddr
alaIpDirectedBroadcastCtrlDstMask
alaIpDirectedBroadcastCtrlVlanID
```

ip directed-broadcast clear

Clears all the trusted information configured.

ip directed-broadcast clear

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> ip directed-broadcast clear
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

ip directed-broadcast	Enables or disables IP directed broadcasts routed through the switch.

MIB Objects

```
alaIpDirectedBroadcastCtrlTable
```

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 6450, 6350

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	Status
ftp	21	enabled
ssh	22	enabled

service name	port	Status
telnet	23	enabled
udp-relay	67	enabled
http	80	enabled
network-time	123	enabled
snmp	161	enabled
secure-http	443	enabled

Examples

```
-> ip service all
-> ip service ftp telnet snmp
-> ip service port 1024
-> no ip service ftp snmp
-> no ip service all
```

Release History

Release 6.6.3; 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 tables

This command is used to obtain the space to extend the number of IPv4 interfaces and IPv4 static routes supported on the switch by reducing the number of IPv6 neighbor entries.

ip tables {extend | default}

Syntax Definitions

extend	Increase the number of IPv4 interfaces and IPv4 static routes to 32 and 64 respectively.
default	Enable default allocation of IPv4 interfaces and IPv4 static routes.

Defaults

By default, 8 interfaces, 8 static routes, and 96 IPv6 neighbor entries are supported.

Platforms Supported

OmniSwitch 6350

Usage Guidelines

- Use this command to extend the number of IPv4 interfaces and IPv4 static routes to 32 and 64 respectively by reducing the number of IPv6 neighbor entries to 76.
- After using this command, save the configurations using the **write memory** command and reload the switch to reflect the revised space allocation for interface and static routes.
- If the number of interfaces or static routes are already configured to 8, **default** option cannot be used.
- If more than 76 static IPv6 neighbor entries are already configured, **extend** option cannot be used.

Examples

```
-> ip tables extend
-> ip tables default
```

Release History

Release 6.7.2.R04; command introduced.

Related Commands

ip interface	Configures an IP interface to enable IP routing on a VLAN.
ip static-route	Creates or deletes an IP static route.

MIB Objects

```
alaIptablesLimitConfig
```

ip redist

Controls the conditions for redistributing IPv4 routes between different protocols.

ip redist {local | static | rip} into {rip} route-map *route-map-name* **[status {enable | disable}]**

no ip redist {local | static | rip} into {rip} [route-map *route-map-name***]**

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
rip	Specifies RIP as the source or destination 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 6450, 6350

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.

Examples

```
-> ip redist rip into static route-map rip-to-static1
-> ip redist rip into static route-map rip-to-static2
-> no ip redist rip into static route-map rip-to-static2
-> ip redist static into rip route-map static-to-rip
-> ip redist static into rip route-map static-to-rip disable
```

Release History

Release 6.6.3; command introduced.

Related Commands

show ip redist	Displays the route map redistribution configuration.
ip route-map action	Creates a route map for redistribution and sets the status of the route map to permit or deny.

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. The access list name can have a maximum length of 20 characters.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.3; 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 for redistribution.
deny	Denies the IP 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 the 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**

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.

Note. 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 6.6.3; 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 redistribution and sets the status 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 valid range is 1 to 100.
permit	Permits route redistribution.
deny	Denies route redistribution.

Defaults

parameter	default
number	50
permit | deny	**permit**

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.3; 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 redistributed.
all-subnets	Redistributes all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Redistributes only the 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 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 6450, 6350

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.

Note. Configuring the combination of **redist-control aggregate** with **action 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 redistributed. If the best matching address is type **permit** and the route map action is **deny,** the route is not redistributed.
- 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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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 {***access-list-name* **|** *ipv6_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.
ipv6_address/prefixLen	The destination IPv6 address along with the prefix length of the routes to be redistributed.
all-subnets	Redistributes all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Redistributes only the 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 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 6450, 6350

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.

Note. Configuring the combination of **redist-control aggregate** with **action 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 redistributed. If the best matching address is type **permit** and the route map action is **deny,** the route is not redistributed.
- 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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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 6450, 6350

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 redistributed. If the best matching nexthop is type **permit** and the route map action is **deny,** the route is not redistributed.
- 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 6.6.3; 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 for redistribution 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 6450, 6350

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 redistributed. If the best matching nexthop is type **permit** but the route map action is **deny,** the route is not redistributed.
- 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 6.6.3; 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 for redistribution 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*

no ip route-map *route-map-name* **[sequence-number** *number***] match 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	The tag number.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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 interface name of the route outgoing interface.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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 interface name of the route outgoing interface.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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 6450, 6350

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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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	Redistributes the actual metric value. The configured metric value is ignored. Use any value except 0.

Defaults

parameter	default
number	50

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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 route being distributed.

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 6450, 6350

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** must 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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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 6450, 6350

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** must 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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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 6450, 6350

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** must 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 6.6.3; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution 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
```

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]**

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 must act as an alias (or proxy) for this IP address. When the alias option is used, the switch responds to all ARP requests for the specified IP address with its own MAC address. You can also enable the proxy feature for an IP interface using the **ip interface** command. When enabled, ARP requests return the MAC address of the IP router interface and all traffic within the VLAN is routed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to delete a permanent ARP entry.

Note. Using the **arp alias** command is not related to proxy ARP as defined in RFC 925. Confguring **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.

- Since 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 6.6.3; 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 6450, 6350

Usage Guidelines

- This commands only clears dynamic entries. If permanent entries are added to the table, they must be removed using the **no** form of the **ip service** command.
- Dynamic entries remain in the ARP table until they time out. The switch uses the MAC Address table timeout value as the ARP timeout value. Use the **mac-address-table aging-time** command to set the timeout value.

Examples

```
-> clear arp-cache
```

Release History

Release 6.6.1; command introduced.

Related Commands

ip service	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 6450, 6350

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 6.6.1; 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 determines if ARP Request packets containing a specific IP address are processed or discarded by the switch.

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 6450, 6350

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 6.6.1; 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 filter	Displays the ARP filter configuration.

MIB Objects

```
alaIpArpFilterTable
   alaIpArpFilterIpAddr
   alaIpArpFilterIpMask
   alaIpArpFilterVlan
   alaIpArpFilterMode
   alaIpArpFilterType
```

clear arp filter

Clears the ARP filter database of all entries.

clear arp-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command introduced.

Related Commands

arp filter	Configures an ARP filter to allow or block the processing of specified ARP Request packets.
show arp filter	Displays the ARP filter configuration.

MIB Objects

```
alaIpClearArpFilter
```

ip arp-limit default

This command is used to change the ARP mode from extend to default mode.

ip arp-limit default

Syntax Definitions

N/A

Defaults

Default ARP mode can store a total of 512 entries in switch and the ECMP limit is 4.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use this command to change the ARP mode from extend to default mode.
- Only Static and Dynamic ARP entries are stored in hardware table and the maximum limit is a combination of Static and Dynamic ARP entries.
- Make sure that less than 512 are static ARP entries configured on switch, when changing ARP mode from extend to default.
- After using this command, save the configurations using the **write memory** command and reload the switch, to reflect the ARP mode changes in the switch.

Examples

```
-> ip arp-limit default
```

Release History

Release 6.6.5; command introduced.

Related Commands

ip arp-limit extend	This command is used to change the ARP mode from default to extend mode.

MIB Objects

N/A

ip arp-limit extend

This command is used to change the ARP mode from default to extend mode.

ip arp-limit extend

Syntax Definitions

N/A

Defaults

Extend ARP mode can store a total of 1024 entries in switch and the ECMP limit is 2.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use this command to change the ARP mode from default to extend mode.
- Only Static and Dynamic ARP entries are stored in hardware table and the maximum limit is a combination of Static and Dynamic ARP entries.
- After using this command, save the configurations using the **write memory** command and reload the switch, to reflect the ARP mode changes in the switch.

Examples

```
-> clear arp filter
```

Release History

Release 6.6.5; command introduced.

Related Commands

ip arp-limit default	This command is used to change the ARP mode from extend to default mode.

MIB Objects

N/A

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. The type value along with the ICMP code determines the category of ICMP message being specified.
code	The ICMP code type. The ICMP code used in conjunction with the ICMP type determines the category 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 6450, 6350

Usage Guidelines

- This command allows the use 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 as follows:

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 message, some of the more common ICMP messages have their own CLI commands, as described in the following pages. 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 are not recommended as it can cause the switch instability. The switch can become unstable due to high-CPU conditions due to high volume of traffic caused 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 enables, disables, or sets 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 6.6.1; 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 6450, 6350

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, enables, disables, or sets 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 6.6.1; 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 add-mask [request | reply] {{enable | disable} | min-pkt-gap *gap***}**

Syntax Definitions

request	Specifies request address mask messages.
reply	Specifies reply address mask messages.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
gap	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable | disable	**enable**
gap	0

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- A gateway receiving an address mask request must 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, enables, disables, or sets 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 6.6.1; 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> icmp messages enable
-> icmp messages disable
```

Release History

Release 6.6.1; 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
```

twamp server

Configures a TWAMP server on the switch.

twamp server [port *port-number***] [inactivity-timeout** *mins***] [allowed-client** *ipv4-address ip-mask***]**

no twamp server

Syntax Definitions

port	The TCP port on which the TWAMP server will listen for the client connection or requests. The TCP port can be configured in the range 30000 to 30999.
inactivity-timeout	The inactivity timer (in minutes) for the control session in case no packets are received in the established session. The timer can be configured in the range 1 to 30. The session is closed if no packets are received within the configured inactivity-timeout period.
allowed-client	The client IP address or range and mask which shall be allowed to establish connection with the server. Upto 32 client IPs can be configured.

Defaults

parameter	default
port	862
inactivity-timeout	15

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- When TWAMP server is configured on the switch, the loopback0 IP address will be taken as the IP address of the server.
- Only one TWAMP server can be configured on a switch at a given point of time.
- When TWAMP server port is reconfigured, a system reload is needed for the reconfigured port to come into effect.
- Maximum 32 control sessions are allowed per switch. A control sessions can have 128 test sessions.
- When configuring large number of test sessions, the timeout value should be configured in the client side such that there is enough gap between multiple test session timeouts to avoid interrupts and loss of messages at interrupt level.
- Use the **no** form of this command to remove the TWAMP server configuration.

Examples

```
-> twamp server port 30333 inactivity-timeout 20 allowed-client 172.16.1.1/16
-> no twamp server
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

show twamp server info	Displays the configuration details of the TWAMP server on the switch.
show twamp server connections	Displays the TWAMP Client connections established with the TWAMP server on the switch at a given point of time. The TWAMP connections can also be viewed for a specific client.

MIB Objects

```
alcatelIND1TWAMP
   twampServerTable
   twampPortNumber
   twampInactivityTimeout
   twampClientIpaddress
   twampClientIpaddressMask
```

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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 values that are added together. The commands for setting the packet penalty value are the **twamp server**, **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 6.6.1; command introduced.

Related Commands

twamp server	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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 member port 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 includes statistics regarding the spoofed traffic.

Note. 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

Event        Source       Total        Last 33 seconds
-------------+-------+------------+-----------------------
spoof         5/26   18           2          last mac 00:08:02:e2:17:70
```

output definitions

Total	Total number of input datagrams received including datagrams 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 local-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. Typically, this value must 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 had 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 value is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragmented	Number of successfully fragmented IP datagrams.
Fragment failed	Number of packets received and discarded by IP because they could not be fragmented. This situation could happen if a large packet has the “Don’t Fragment” flag set.
Forwarded	Number of IP datagrams forwarded by the switch.
Generated	Total number of IP datagrams that local IP user protocols (including ICMP) generated in response to requests for transmission. This does not include any datagrams counted as “Forwarded.”

output definitions (continued)

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. Forwarded packets are also counted if they are discarded. It also includes any datagrams that a host cannot route because all of its default routers are down.
Fragments generated	The of IP datagram fragments generated as a result of fragmentation.
Routing entry discards	Number of packets received and discarded by IP even though no problems were encountered to prevent their transmission to their destination (for example, discarded because of lack of buffer space).
Event	The type of event (**spoof**).
Source	The slot and port number of the port that has received spoofed packets and is also a member of the UserPorts group. Ports are configured as members of the UserPorts group through the **policy port group** command.
Total	The total number of spoofed packets received on the source port.
Last *xx* **seconds**	The number of spoofed packets blocked in the last number of seconds indicated. Also includes the source MAC address of the last spoofed packet received.

Release History

Release 6.6.1; command introduced.

Related Commands

show icmp statistics	Displays ICMP statistics and errors.

show ip interface

Displays the status and configuration of IP interfaces.

show ip interface [*name* | **vlan** *vlan id* | **dhcp-client]**

Syntax Definitions

name	The name associated with the IP interface.
vlan_id	VLAN ID (displays a list of IP interfaces associated with the VLAN).
dhcp-client	Displays the configuration and status of the DHCP-Client interface.

Defaults

By default, all IP interfaces are displayed.

Platforms Supported

OmniSwitch 6450, 6350

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 the list of interfaces configured for the specified VLAN.
- Specify an optional interface *name* to display detailed information about an individual interface.

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
firewall            11.1.1.1        255.0.0.0           UP     YES firewall 173

gbps                5.5.5.5         255.255.255.0     DOWN      NO vlan 7
if222               30.1.5.1        255.0.0.0           UP     YES vlan 222
ldap_client1        173.22.16.115   255.255.255.0       UP     YES vlan 173
ldap_server1        174.22.16.115   255.255.255.0       UP     YES vlan 174
radius_client3      110.1.1.101     255.255.255.0       UP     YES vlan 30
vlan-2              0.0.0.0         0.0.0.0           DOWN      NO unbound
vlan-23             23.23.23.1      255.255.255.0       UP     YES vlan 23
```

output definitions

Name	Interface name. Generally, the name configured for the interface is specified (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. 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 = dhcp-client
  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,
  Encapsulation                  =   eth2,
  Forwarding                     =   disabled,
  Administrative State           =   enabled,
  Operational State              =   up,
  Operational State Reason       =   unbound,
  Router MAC                     =   00:d0:95:6a:f4:55,
  Local Proxy ARP                =   disabled,
  Maximum Transfer Unit          =   1500,
```

```
 Primary (config/actual)        =   yes/yes,
 Vsi Accept Filter              =   "alcatel.a4400.0"
 Server Preference              =   Disabled
DHCP-CLIENT Parameter Details
 Client Status                  =   Active,
 Server IP                      =   198.206.181.55,
 Router Address                 =   N.A.,
 Lease Time Remaining           =   2 Days 10 Hours 20 Min,
 Option-60                      =   Option60_example,
 HostName                       =   TechPubs,
 Time Zone                      =   0
```

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. 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 source IP address is invalid. • **tunnel-dst-unreachable—**Tunnel destination IP address is not reachable. **Note:** The **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. **Note:** 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.
Server Preference	Indicates if the DHCP server preference option is enabled or disabled.

output definitions (continued)

DHCP-CLIENT Parameter Details	(The following parameters are only applicable to the 'dhcp-client' interface)
Client Status	DHCP Client Status (**In-active**, **Active**)
Server IP	The IP address of the DHCP server.
Lease Time Remaining	The lease time remaining for the DHCP client IP address.
Option-60	The option-60 string that shall be included in DHCP discover or 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,
```

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. 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 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**).

output definitions (continued)

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 source IP address is invalid. • **tunnel-dst-unreachable—**Tunnel destination IP address is not reachable. **Note:** 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 6.6.1; command was introduced.
Release 6.6.2; DHCP Client options added.
Release 6.6.4; Vsi Accept Filter field added in output.
Release 6.7.2.R04; server preference field added in output.

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.
show icmp statistics	Displays ICMP statistics and errors.

MIB Objects

```
alaIpInterfaceTable
   alaIpInterfaceName
   alaIpInterfaceAddress
   alaIpInterfaceMask
   alaIpInterfaceAdminState
   alaIpInterfaceDeviceType
   alaIpInterfaceVlanID
   alaIpInterfaceIpForward
   alaIpInterfaceEncap
   alaIpInterfaceLocalProxyArp
   alaIpInterfacePrimCfg
   alaIpInterfaceDhcpVsiAcceptFilterString
   alaIpInterfaceOperState
   alaIpInterfaceOperReason
   alaIpInterfaceRouterMac
   alaIpInterfaceBcastAddr
   alaIpInterfacePrimAct
   alaIpInterfaceMtu
   alaIpInterfaceTunnelSrc
```

```
alaIpInterfaceTunnelDst
```

show ip interface cvlan

Displays the SVLAN to CVLAN mapped interfaces.

show ip interface cvlan

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ip interface cvlan
NameIP    AddressSubnet   Mask         Status   Forward  Device      CVLAN
--------------------------------------------------------------------------------
v10       10.10.10.2      255.255.255.0  UP     YES      vlan 1000    10
```

Release History

Release 6.6.5; command introduced.

Related Commands

Ip interface cvlan	Configures the SVLAN interface using which the SVLAN can be mapped to the CVLAN.

MIB Objects

N/A

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 6450, 6350

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               -
 telnet            management
 ssh               -
 tftp              -
 ldap-server       -
 radius            -
 snmp              -
 ftp               -
```

Release History

Release 6.6.1; 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.

show ip route [summary]

Syntax Definitions

summary	Displays a summary of routing protocols that appear in the IP Forwarding table.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The IP Forwarding table includes static routes as well as all routes learned through routing protocols (for example, RIP).
- Use the optional **summary** keyword to display a list of routing protocols and the number of routes for each protocol that appear in the IP Forwarding table.

Examples

```
-> show ip route

+ = Equal cost multipath routes
 Total 4 routes

  Dest Address      Subnet Mask       Gateway Addr      Age       Protocol
------------------+-----------------+-----------------+---------+-----------
  0.0.0.0           0.0.0.0           10.255.11.254     01:50:33  NETMGMT
  10.255.11.0       255.255.255.0     10.255.11.225     01:50:33  LOCAL
  127.0.0.1         255.255.255.255   127.0.0.1         01:51:47  LOCAL
  212.109.138.0     255.255.255.0     212.109.138.138   00:33:07  LOCAL

-> show ip route summary

  Protocol        Route Count
----------------+--------------
  All                      4
  Local                    3
  Netmgmt                  1
  RIP                      0
  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.
Route Count	The number of routes that appear in the IP Forwarding table for each protocol type listed.

Release History

Release 6.6.1; command introduced.

Related Commands

ping	Used to test whether an IP destination can be reached from the local switch.
traceroute	Used to find the path taken by an IP packet from the local switch to a specified destination.
show ip route	Displays a list of all routes (static and dynamic) that exist in the IP router database.

MIB Object

N/A

show ip route-pref

Displays the IPv4 routing preferences of a router.

show ip route-pref

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ip route-pref
  Protocol    Route Preference Value
------------+-----------------------
  Local                 1
  Static                2
```

Release History

Release 6.6.1; command introduced.

Related Commands

ip route-pref	Configures the route preference of a router.

MIB Objects

```
alaIprmRtPrefTable
  alaIprmRtPrefLocal
  alaIprmRtPrefStatic
  alaIprmRtPrefRip
```

show ip redist

Displays the IPv4 route map redistribution configuration.

show ipv6 redist [rip]

Syntax Definitions

rip	Displays route map redistribution configurations that use RIP as the destination (into) protocol.

Defaults

By default all route map redistribution configurations are shown.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Specify a destination protocol with this command to display only the configurations that redistribute routes into the specified protocol.

Release History

Release 6.6.1; command introduced.

Examples

```
-> show ip redist

Source       Destination
Protocol     Protocol     Status    Route Map
-------------+------------+---------+--------------------
RIP          Static         Enabled   ipv4rm

-> show ip redist rip

Source       Destination
Protocol     Protocol     Status    Route Map
-------------+------------+---------+--------------------
Static          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.

output definitions

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 6450, 6350

Usage Guidelines

If the *access-list-name* is not specified in this command, all the access lists are 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 6.6.1; 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 6450, 6350

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 6.6.1; command introduced.

Related Commands

ip route-map action	Creates a route map for redistribution and sets the status of 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.

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 for redistribution and where duplicate routes are compared to determine the best route to use. If a route does not appear in the IP router database list, then the switch does not know about it. In the case of dynamically learned routes, this could indicate that the route was never received by the switch.

show ip router database [protocol *type* | **gateway** *ip_address* | **dest {***ip_address/prefixLen* | *ip_address***}]**

Syntax Definitions

type	Routing protocol type (local, static, or RIP).
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 6450, 6350

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 the 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, the protocol determines precedence. Local routes are given the highest level of precedence followed by static, then RIP 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
Destination         Gateway          Protocol Metric VLAN
------------------+----------------+--------+------+-----
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
143.209.92.0/24     172.28.6.254     STATIC   1      N/A
172.28.6.0/24       172.28.6.2       LOCAL    1      6

Inactive Static Routes

Destination       Gateway        Metric
-----------------+--------------+------
1.0.0.0/8          8.4.5.3         1
```

output definitions

Destination	Destination IP address. Also includes the mask prefix length notation after the address to indicate the subnet mask value. For example, **/24** indicates the destination IP address has a 24-bit mask (255.255.255.0).
Gateway	IP address of the gateway from which this route was learned.
Protocol	Protocol by which this IP address was learned: LOCAL, STATIC, RIP).
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. N/A** appears in this field for static routes as they are not learned on a VLAN.

Release History

Release 6.6.1; command introduced.

Related Commands

show ip route	Displays the IP Forwarding table.

MIB Object

N/A

show ip config

Displays IP configuration parameters.

show ip config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The **show ip config** command displays the source IP address, destination IP address, and VLAN information of the control directed-broadcast. Each row will have each source IP address, destination IP address, and VLAN information defined. The non-defined parameters will be mentioned as '-'. The show output displays all the configured control directed broadcast entries irrespective of the IP directed broadcast mode.

Examples

```
-> show ip config
ip directed-broadcast   =   controlled,
Control Directed Broadcast Entries
Source-ip/mask = 10.10.10.1 / 0.0.0.0,
  Destination-ip/mask = 10.10.10.2 / 0.0.0.0;
  10.10.10.3 / 0.0.0.0;
  25.25.26.2 / 0.0.0.0,
  vlan = 2;
  6

Source-ip/mask = 20.20.20.1 / 0.0.0.0,
  Destination-ip/mask = -,
  vlan = -

IP default TTL          =   64
```

output definitions

IP directed-broadcast	Indicates whether the IP directed-broadcast feature is on, off, or controlled.
Source-ip/mask	Trusted source IP address and mask configured for control directed broadcast.
Destination-ip/mask	Trusted destination IP address and mask configured for control directed broadcast.

output definitions

VLAN	Trusted VLAN ID configured for control directed broadcast.
IP default TTL	The default TTL value for IP packets.

Release History

Release 6.6.1; command introduced.
Release 6.7.1 R02; Control Directed Broadcast Entries fields added.

Related Commands

ip directed-broadcast	Enables or disables IP directed broadcasts routed through the switch.
ip directed-broadcast allow	Specify the source IP address, destination IP address, and VLAN information to broadcast the packets in controlled manner.
ip default-ttl	Sets TTL value for IP packets.

N/A

show ip protocols

Displays switch routing protocol information and status.

show ip protocols

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

This command also displays the switch 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,

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.
Debug level	What the current router debug level is.
Debug sections	What types of debugging information are being tracked.

Release History

Release 6.6.1; 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 6450, 6350

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
secure_http               443   enabled
```

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 6.6.1; 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 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 6450, 6350

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)

 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
 10.255.11.25      00:b0:d0:42:80:24   DYNAMIC               3/20  vlan 1
 10.255.11.26      00:b0:d0:42:82:59   DYNAMIC               3/20  vlan 1
 10.255.11.254     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
Port	The port 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 6.6.3; 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
   alaIpNetToMediaAuth
```

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 6450, 6350

Usage Guidelines

- OmniSwitch provides the proxy-arp functionality for the addresses contained in this table.
- Dynamic-proxy-arp is used in conjunction 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	The IP address of the router.
Hardware Addr	The MAC address of the router.
VLAN	The VLAN the entry is learned on.
Interface	The interface the entry is learned on.

Release History

Release 6.6.3; 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 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 6450, 6350

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 6.6.1; 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 6450, 6350

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. The type value along with the ICMP code specify the variety of ICMP message.
Code	The ICMP message code. The code value along with the ICMP type specify the variety 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 6.6.1; 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.

MIB Object

```
N/A
```

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.

show icmp [statistics]

Syntax Definitions

statistics	Optional syntax.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the ICMP Table to monitor and troubleshoot the switch.
- If an ICMP message cannot be delivered, a second message is not generated. This is to avoid an endless flood of ICMP messages.

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 counts all the messages.
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).

output definitions (continued)

Destination unreachable	Number of “destination unreachable” messages that were sent/received by the switch.
Time exceeded	Number of “time exceeded” messages that were sent/received by the switch. These messages are generated when a packet is dropped and the TTL counter reaches zero. When a large number of **Time exceeded** messages occur, it implies that the packets are looping and the 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 IP software or possibly the gateway software.
Source quench	Number of messages sent/received that tell a host that it is sending too many packets. A host must 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 6.6.1; command introduced.

Related Commands

show udp statistics	Displays UDP errors and statistics.

MIB Object

N/A

show twamp server info

Displays the configuration details of the TWAMP server on the switch.

show twamp server info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

This command displays TWAMP server information only if TWAMP server is configured on the switch, else an error message is displayed.

Examples

```
-> show twamp server info
TWAMP Server
Port: 30333
Inactivity timeout: 20 mins
Allowed-Client: 172.16.1.1/16
```

output definitions

Port	Displays the TCP port on which the server is listening.
Inactivity timeout	Displays the time to wait in minutes if no packet associated with the connection is received.
Allowed-Client	Displays the client IP or range and mask which shall be allowed to establish connection with the server.

```
-> show twamp server info
ERROR: No Twamp server configured
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

twamp server	Configures a TWAMP server on the switch.

MIB Object

```
twampServerTableEntry
   twampPortNumber
   twampInactivityTimeout
   twampClientIpaddress
```

show twamp server connections

Displays the TWAMP client connections established with the TWAMP server on the switch at a given point of time. The TWAMP connections can also be viewed for a specific client.

show twamp server connections [client *ipv4-address***]**

Syntax Definitions

client	Specify the TWAMP client IP to view the specific client session details for that client.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- To view the TWAMP client connections for a specific client, specify the client IP address. The information is displayed if the connection exists.
- The client connections are displayed only for the established sessions. Other intermediate connection status for greeting sent and setup response is not displayed in the CLI output.
- The statistics details for the established connections is updated every two minutes.
- The statistics for maximum of 128 test sessions after the timeout value from the client side is updated with the connection status as “ENDED”.

Examples

```
-> show twamp server connections client 200.200.1.1
Client IP   Conn Status    Time of Last Run          Pkts Sent   Pkts Received     Session Identifier
-------------------------------------------------------------------------------------------------------
200.200.1.1 SETUP_DONE     THU OCT 08 2015  19:39:13 10          10                2eb0b7b6a5c405df
200.200.1.1 SETUP_DONE     THU OCT 08 2015  19:39:13 10          10                2eb0b7b6fe7fb742
```

output definitions

Client IP	Displays the IP address of the TWAMP client connected to the TWAMP server.
Conn Status	Displays the connection status of the TWAMP client. The connection status is displayed as SETUP_DONE when the control connection is established and the test sessions are started. Other intermediate connection status for greeting sent and setup response is not displayed.
Time of Last Run	Displays the time details of the TWAMP client session when it was last run.
Pkts Sent	Displays the number of packets sent during the TWAMP client session.

output definitions

Pkts Received	Displays the number of packets received during the TWAMP client session.
Session Identifier	Displays the session ID for the TWAMP client session.

Release History

Release 6.7.1 R02; command introduced.

Related Commands

twamp server	Configures a TWAMP server on the switch.
show twamp server info	Displays the configuration details of the TWAMP server on the switch.

MIB Object

```
twampServerConnectionTable
   twampServerConnClientIP
   twampServerConnSessionId
   twampServerConnTimeOfLastRun
   twampServerConnPktsSent
   twampServerConnPktsRecvd
   twampServerConnectionStatus
```

show tcp statistics

Displays TCP statistics.

show tcp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 the segments 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 the segments available 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 the TCP connections have been reset from the "Established" or "Close Wait" state to the “Closed” state.

Release History

Release 6.6.1; command introduced.

Related Commands

show icmp statistics	Displays ICMP statistics and errors.
show tcp ports	Displays the TCP connection table.

MIB Object

N/A

show tcp ports

Displays the TCP connection table.

show tcp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command introduced.

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.
show twamp server info	Displays TCP statistics.

MIB Object

N/A

show udp statistics

Displays UDP errors and statistics.

show udp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command introduced.

Related Commands

show udp ports	Displays the UDP Listener table.

MIB Object

N/A

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 6450, 6350

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 6.6.1; command introduced.

Related Commands

show udp statistics	Displays UDP errors and statistics.

MIB Object

N/A

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 6450, 6350

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 value 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 value 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 **twamp server** 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 value 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 value is set using the **ip dos scan udp open-port-penalty** command.

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

- This command displays the number of attacks the switch has detected for several types of DoS attacks.
- Just because an attack is detected and reported, doesn't necessarily mean an attack occurred. The switch assumes 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 6.6.1; 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 6450, 6350

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 6.6.1; command introduced.

Related Commands

ip dos arp-poison restricted-address	Adds or deletes an ARP Poison restricted address.

MIB Objects

```
alaDoSArpPoisonTable
   alaDoSArpPoisonIpAddr
   alaDoSArpPoisonDetected
```

35 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 dad-check** **ipv6 hop-limit** **ipv6 pmtu-lifetime** **ipv6 host** **ipv6 neighbor stale-lifetime** **ipv6 neighbor** **ipv6 prefix** **ipv6 route** **ipv6 static-route** **ipv6 route-pref** **ipv6 ra-filter** **ipv6 ra-filter clear counters** **ping6** **traceroute6** **show ipv6 hosts** **show ipv6 icmp statistics** **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 udp ports** **show ipv6 information** **show ipv6 ra-filter vlan** **show ipv6 ra-filter counters**
IPv6 Route Map Redistribution	**ipv6 redist** **ipv6 access-list** **ipv6 access-list address** **show ipv6 redist** **show ipv6 access-list**
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.

ipv6 interface *if_name* **vlan** *vid* **[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.
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 - 1800.
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 - 3600000. 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 9000 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 6450, 6350

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 interfaces must have a name.
- When creating an IPv6 interface you must specify a VLAN ID. 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.
- To enable IPv6 routing you must first create a VLAN, then create an IPv6 interface on the VLAN. See Chapter 25, "VLAN Management Commands," for information on creating VLANs.

Examples

```
-> ipv6 interface Test vlan 1
-> no ipv6 interface Test
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show ipv6 interface	Displays IPv6 Interface Table.

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. 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 6450, 6350

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 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 25, “VLAN Management Commands,” for information on creating VLANs.

Examples

```
-> ipv6 address 4132:86::19A/64 Test_Lab
-> ipv6 address 2002:d423:2323::35/64 Test_Engr
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show ipv6 interface	Displays IPv6 Interface Table.

MIB Objects

```
IPv6IfIndex
alaIPv6InterfaceAddressTable
   alaIPv6InterfaceAddress
   alaIPv6InterfaceAddressAnycastFlag
   alaIPv6InterfaceEUI64AddressPrefixLength
   alaIPv6InterfaceEUI64AddressrowStatus

For EUI-64 Addresses:
alaIPv6InterfaceEUI64AddresssTable
   alaIPv6InterfaceEUI64Address
   alaIPv6InterfaceEUI64AddressPrefixLength
   alaIPv6InterfaceEUI64AddressRowStatus
```

ipv6 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIPv6InterfaceAddressTable
   alaIPv6InterfaceAddressDADStatus
```

ipv6 hop-limit

Configures the value placed in the hop limit field in the header of all IPv6 packets that are originated by the switch. It also configures the value placed in the hop limit field in router advertisements.

ipv6 hop-limit *value*

no ipv6 hop-limit

Syntax Definitions

value	Hop limit value. The range is 0 - 255.

Defaults

parameter	default
value	64

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> ipv6 pmtu-lifetime 30
```

Release History

Release 6.6.1; command was 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 6450, 6350

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 6.6.1; command was 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> ipv6 neighbor stale-lifetime 1400
```

Release History

Release 6.6.1; command was 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 (e.g., 00:00:39:59:F1:0C).
if_name	Name assigned to the interface on which the neighbor resides.
slot/port	Slot/port used to reach the neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was 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, i.e. time until deprecation. A value of 4294967295 represents infinity.
preferred-lifetime *time*	Length of time, in seconds, that this prefix will remain preferred, i.e. time until deprecation. A value of 4294967295 represents infinity.
on-link-flag	On-link configuration flag. When “true” this prefix can be used for on-link determination.
autonomous-flag	Autonomous address configuration flag. When “true”, indicates that this prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
if_name	Name assigned to the interface.

Defaults

parameter	default
valid-lifetime *time*	2592000
preferred-lifetime *time*	604800
on-link-flag	true
autonomous-flag	true

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use the **no** form of this command to delete a prefix.

Examples

```
-> ipv6 prefix 4132:86::/64 Test
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show ipv6 prefixes	Displays IPv6 prefixes used in router advertisements.

MIB Objects

```
IPv6IfIndex
alaIPv6InterfacePrefixTable
   alaIP6vInterfacePrefix
   alaIP6vInterfacePrefixLength
   alaIP6vInterfacePrefixValidLifetime
   alaIP6vInterfacePrefixPreferredLifetime
   alaIP6vInterfacePrefixonLinkFlag
   alaIP6vInterfacePrefixAutonomousFlag
   alaIP6vInterfacePrefixRowStatus
```

ipv6 route

Configures a static entry in the IPv6 route. *This command is currently not supported. Please use the new* **ipv6 static-route** *command.*

ipv6 route *ipv6_prefix/prefix_length ipv6_address* **[***if_name***]**

no ipv6 route *ipv6_prefix/prefix_length ipv6_address* **[***if_name*]

Syntax Definitions

ipv6_prefix	IPv6 network that is the destination of this static route.
/prefix_length	The number of bits that are significant in the iPv6 address (mask). (0...128).
ipv6_address	IPv6 address of the next hop used to reach the specified network.
if_name	If the next hop is a link-local address, the name of the interface used to reach it.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use the **no** form of this command to remove a static route.

Examples

```
-> ipv6 route 212:95:5::/64 fe80::2d0:95ff:fe6a:f458 v6if-137
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show ipv6 routes	Displays IPv6 Forwarding Table.

MIB Objects

```
alaIPv6StaticRouteTable
   alaIPv6StaticRouteNextHop
   alaIPv6StaticRouteIfIndex
   alaIPv6StaticRouteDest
   alaIPv6StaticRoutePrefixLength
   alaIPv6StaticRouteRowStatus
```

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***]**

no ipv6 static-route *ipv6_prefix/prefix_length* **gateway** *ipv6_address* **[***if_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.

Defaults

parameter	default
metric	1

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use the **no** form of this command to remove a static route.

Examples

```
-> ipv6 static-route 212:95:5::/64 gateway fe80::2d0:95ff:fe6a:f458 v6if-137 metric 3
```

Release History

Release 6.6.1; command was introduced.

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
   alaIprmv6StaticRoutePrefixLength
   alaIprmv6StaticRouteNextHop
   alaIprmv6StaticRouteIfIndex
   alaIprmv6StaticRouteMetric
   alaIprmv6StaticRouteRowStatus
```

ipv6 route-pref

Configures the route preference of a router.

ipv6 route-pref {static | rip} *value*

Syntax Definitions

static	Configures the route preference of static routes.
rip	Configures the route preference of RIPng routes.
value	Route preference value.

Defaults

parameter	default
static *value*	2
rip *value*	120

Platforms Supported

OmniSwitch 6450, 6350

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 static 2
-> ipv6 route-pref rip 60
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show ipv6 route-pref	Displays the configured route preference of a router.

MIB Objects

```
alaIprmRtPrefTable
   alaIprmRtPrefLocal
   alaIprmRtPrefStatic
   alaIprmRtPrefRip
```

ipv6 ra-filter

Configures the Router Advertisement (RA) filtering on an IPv6 VLAN. When RA filtering is enabled on a VLAN, router advertisements received on any port or linkagg are discarded. If one or more trusted ports or linkaggs are configured, RAs received on them will be accepted and sent on to any connected IPv6 nodes.

ipv6 ra-filter vlan *vlan-number* **[{trusted-port** *slot/port* **| trusted-linkagg** *id***}]**

Syntax Definitions

vlan-number	Specify the VLAN on which RA filtering is being configured.
slot/port	Specify a trusted port.
linkagg *id*	Specify a trusted linkagg.

Defaults

- By default, RA filtering feature is disabled.
- By default, all ports and linkaggs are untrusted.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to disable RA filtering on a VLAN.
- RAF will only allow filtering of router advertisements on a per-port basis.
- A maximum of 32 VLANs can be configured for RA filtering.
- RA filtering feature cannot be enabled on VLAN which is used as a openflow VLAN, Ethernet service VLAN and as a IPMvlan and vice-versa.
- RA filtering feature cannot be enabled on port which is a mirrored port and openflow enabled port and vice-versa.

Examples

```
-> ipv6 ra-filter vlan 5
-> ipv6 ra-filter vlan 5 trusted-port 1/22
-> ipv6 ra-filter vlan 5 trusted-linkagg 2
```

The following command returns port 1/22 to the untrusted state.

```
-> no ipv6 ra-filter vlan 5 trusted-port 1/22
```

The following command disables RA filtering on VLAN 5.

```
-> no ipv6 ra-filter vlan 5
```

Release History

Release 6.7.1; command introduced.

Related Commands

ipv6 ra-filter clear counters	Clear the router advertisement filtering counter statistics.
show ipv6 ra-filter vlan	Displays the list of VLANs configured for RA filtering.
show ipv6 ra-filter counters	Displays the counter statistics of the NIs which are up.

MIB Objects

```
alaipv6rafvlantable
   alaIpv6RafVlan
   alaIpv6RafPortIfIndex
```

ipv6 ra-filter clear counters

Clear the router advertisement filtering counter statistics.

ipv6 ra-filter clear counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> ipv6 ra-filter clear counters
```

Release History

Release 6.7.1; command introduced.

Related Commands

show ipv6 ra-filter counters	Displays the counter statistics of the NIs which are up.

MIB Objects

```
alaIPv6Config
   alaIPv6ClearRafCounters
```

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

traceroute6	Finds the path taken by an IPv6 packet from the local switch to a specified destination.

MIB Objects

N/A

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ping6	Tests whether an IPv6 destination can be reached from the local switch.

MIB Objects

N/A

show ipv6 hosts

Displays IPv6 Local Hosts Table.

show ipv6 hosts [*substring*]

Syntax Definitions

substring	Limits the display to host names starting with the specified substring.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was 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 6450, 6350

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, etc.).

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 6.6.1; command was introduced.

Related Commands

show ipv6 traffic	Displays IPv6 traffic statistics.

MIB Objects

```
ipv6IfIcmpTable
   ipv6IfIcmpInMsgs
   ipv6IfIcmpInErrors
   ipv6IfIcmpInDestUnreachs
   ipv6IfIcmpInAdminProhibs
   ipv6IfIcmpInTimeExcds
   ipv6IfIcmpInParmProblems
   ipv6IfIcmpInPktTooBigs
   ipv6IfIcmpInEchos
   ipv6IfIcmpInEchoReplies
   ipv6IfIcmpInRouterSolicits
   ipv6IfIcmpInRouterAdvertisements
   ipv6IfIcmpInNeighborSolicits
   ipv6IfIcmpInNeighborAdvertisements
   ipv6IfIcmpInRedirects
   ipv6IfIcmpInGroupMembQueries
   ipv6IfIcmpInGroupMembResponses
   ipv6IfIcmpInGroupMembReductions
   ipv6IfIcmpOutMsgs
   ipv6IfIcmpOutErrors
   ipv6IfIcmpOutDestUnreachs
   ipv6IfIcmpOutAdminProhibs
   ipv6IfIcmpOutTimeExcds
   ipv6IfIcmpOutParmProblems
   ipv6IfIcmpOutPktTooBigs
   ipv6IfIcmpOutEchos
   ipv6IfIcmpOutEchoReplies
   ipv6IfIcmpOutRouterSolicits
   ipv6IfIcmpOutRouterAdvertisements
   ipv6IfIcmpOutNeighborSolicits
   ipv6IfIcmpOutNeighborAdvertisements
   ipv6IfIcmpOutRedirects
   ipv6IfIcmpOutGroupMembQueries
   ipv6IfIcmpOutGroupMembResponses
   ipv6IfIcmpOutGroupMembReductions
```

show ipv6 interface

Displays IPv6 Interface Table.

show ipv6 interface [*if_name* | **loopback**]

Syntax Definitions

if_name	Interface name. Limits the display to a specific interface.
loopback	Limits display to loopback interfaces.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If you do not specify an interface name, all IPv6 interfaces are displayed.
- Specify an interface name (e.g., VLAN 12) to obtain 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
loopback            ::1/128                                  Active    loopback
```

output definitions

Name	Interface name. This is usually the VLAN on which the interface is configured.
IPv6 Address/Prefix Length	IPv6 address and prefix length assigned to the interface. If an interface has more than one IPv6 address assigned to it, each address is shown on a separate line.
Status	Interface status (e.g., Active/Inactive).
Device	The device on which the interface is configured (e.g., VLAN 955).

```
-> show ipv6 interface smbif-5

smbif-5
```

```
IPv6 interface index        = 16777216(0x01000000)
Administrative status       = Enabled
Operational status          = Active
  Hardware address              = 00:E0:B1:C2:EE:87
Link-local address(es):
  fe80::2d0:95ff:fe12:f470/64
Global unicast address(es):
  212:95:5::35/64
Anycast address(es):
  212:95:5::/64
Joined group addresses:
  ff02::1:ff00:0
  ff02::2:93da:68lb
  ff02::1
  ff02::1:ff00:35
Maximum Transfer Unit (MTU)   = 1500
Neighbor reachable time (sec) = 538
Base reachable time (sec)     = 360
Retransmit timer (ms)         = 1000
DAD transmits                 = 1
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
RA hop limit                  = 64
RA send MTU option            = No
RA clock skew (sec)           = 600
Packets received            = 215686
Packets sent                = 2019
Bytes received              = 14108208
Bytes sent                  = 178746
Input errors                = 0
Output errors               = 0
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.

output definitions (continued)

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).
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 6.6.1; command was introduced.

Related Commands

ipv6 address	Configures an IPv6 address on a VLAN.
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 6450, 6350

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 6.6.1; command was 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> clear ipv6 pmtu table
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ipv6 pmtu-lifetime	Configures the configure the minimum lifetime for entries in the path MTU Table.
show ipv6 pmtu table	Displays the IPv6 path MTU Table.

MIB Objects

```
alaIPv6ConfigTable
   alaIpv6ClearPMTUTable
```

show ipv6 neighbors

Displays IPv6 Neighbor Table.

show ipv6 neighbors [*ipv6_prefix/prefix_length* | *if_name* | **hw** *hardware_address* | **static]**

Syntax Definitions

ipv6_prefix/prefix_length	IPv6 prefix. Restricts the display to those neighbors starting with the specified prefix.
if_name	Interface name. Restricts the display to those neighbors reached via the specified interface.
hardware_address	MAC address. Restricts the display to the specified MAC address.
static	Restricts display to statically configured neighbors.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

If you do not specify an option (e.g., 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 (e.g., vlan_1)

Release History

Release 6.6.1; command was introduced.

Related Commands

ipv6 neighbor	Configures a static entry in the IPv6 Neighbor Table.

MIB Objects

```
ipv6IfIndex
alaIPv6NeighborTable
   alaIPv6NeighborNetAddress
   alaIPv6NeighborPhysAddress
   alaIPv6NeighborSlot
   alaIPv6NeighborPort
   alaIPv6NeighborType
   alaIPv6NeighborState
```

clear ipv6 neighbors

Removes all entries, except static entries, from IPv6 Neighbor Table.

clear ipv6 neighbors

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was 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 6450, 6350

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
```

output definitions

Name	The interface name. This is usually the VLAN on which the interface is configured.
IPv6 Address/Prefix Length	The IPv6 prefix and prefix length for a Router Advertisement Prefix Option.
Valid Lifetime	Length of time, in seconds, that this prefix will remain valid (i.e., time until deprecation). A value of 4294967295 represents infinity.
Preferred Lifetime	Length of time, in seconds, that this prefix will remain preferred (i.e. time until deprecation). A value of 4294967295 represents infinity.
Flags	**L** - Prefix can be used for onlink determination. **A** - Prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
Source	**config** - Prefix has been configured by management. **dynamic** - Router Advertisements are using interface prefixes.

Release History

Release 6.6.1; command was introduced.

Related Commands

ipv6 prefix	Configures an IPv6 prefix on an interface. Used for configuring prefixes for router advertisements.

MIB Objects

```
IPv6AddrPrefixTable
   IPv6AddressPrefixEntry
   IPv6AddressPrefixLength
   IPv6AddressPrefixLinkFlag
   IPv6AddressPrefixAdvvalidLifetime
   IPv6AddressPrefixAdvPreferredLifetime
alaIPv6InterfacePrefixTable
   alaIPv6InterfacePrefix
   alaIPv6InterfacePrefixLength
   alaIPv6InterfacePrefixValidLifetime
   alaIPv6InterfacePrefixPreferredLifetime
   alaIPv6InterfacePrefixOnLinkFlag
   alaIPv6InterfacePrefixsource
```

show ipv6 routes

Displays IPv6 Forwarding Table.

show ipv6 routes [*ipv6_prefix/prefix_length* | **static]**

Syntax Definitions

ipv6_prefix/prefix_length	IPv6 prefix. Restricts the display to those routes starting with the specified prefix.
static	Restricts display to statically configured routes.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

If you do not specify an option (e.g., “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 Prefix  Gateway Address           Interface         Age          Protocol  Flags
------------------+---------------+--------+-----------------+------------+---------+-----
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
```

output definitions

Destination Prefix	IPv6 destination address and prefix.
Gateway Address	IPv6 address of the gateway used to reach the destination network.
Interface	The IPv6 interface name 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 6.6.1; command was introduced.

Related Commands

ipv6 route	Configures a static entry in the IPv6 route.

MIB Objects

```
IPv6RouteTable
   IPv6Routes
   IPv6RoutesPrefix
   IPV6RoutesStatic
alaIPv6StaticRouteTable
   alaIPv6StaticRouteEntry
```

show ipv6 route-pref

Displays the IPv6 routing preference of the router.

show ipv6 route-pref

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ipv6 route-pref
  Protocol    Route Preference Value
------------+-----------------------
  Local                   1
  Static                  2
  RIP                   120
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ipv6 route-pref	Configures the IPv6 route preference of a router.

MIB Objects

N/A

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, or RIP).
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 6450, 6350

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, then RIP 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
------------------+------------------------+-----------------+---------+-------
195:35::/64         fe80::2d0:95ff:fe12:f470  v6if-to-eagle      RIP       2
212:95:5::/64       fe80::2d0:95ff:fe12:f470  smbif-5            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 IPv6 interface name or loopback.
Protocol	Protocol by which this IPv6 address was learned (LOCAL, STATIC, RIP).
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 6.6.1; command was introduced.

Related Commands

show ipv6 routes	Displays the IPv6 Forwarding Table.

MIB Objects

```
N/A
```

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

show ipv6 udp ports	Displays the UDP Over IPv6 Listener Table.

MIB Objects

```
IPv6TcpConnTable
   IPv6TcpConnEntry
   IPv6TcpConnLocalAddress
   IPv6TcpConnLocalPort
   IPv6TcpConnRemAddress
   IPv6TcpConnRemPort
   IPv6TcpConnIfIndex
   IPv6TcpConnState
```

show ipv6 traffic

Displays IPv6 traffic statistics.

show ipv6 traffic [*if_name*]

Syntax Definitions

if_name	Interface name. Restricts the display to the specified interface instead of global statistics.

Defaults

N/A.

Platforms Supported

OmniSwitch 6450, 6350

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 (e.g., 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 (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes).
Unknown protocol	Number of locally-addressed packets received successfully but discarded because of an unknown or unsupported protocol.
Truncated packets	Number of input packets discarded because the packet frame did not carry enough data.
Local discards	Number of input IPv6 packets for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any packets discarded while awaiting re-assembly.
Delivered to users	Total number of packets successfully delivered to IPv6 user protocols (including ICMP).
Reassembly needed	Number of IPv6 fragments received that needed to be reassembled.
Reassembled	Number of IPv6 packets successfully reassembled.
Reassembly failed	Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.).
Multicast packets	Number of multicast packets received.
Forwarded	Number of output packets that this entity received and forwarded to their final destinations.
Generated	Total number of IPv6 packets that local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any packets counted by the Forwarded statistic.
Local discards	Number of output IPv6 packets for which no problem was encountered to prevent their transmission to their destination, but were discarded (e.g., for lack of buffer space). Note that this counter would include packets counted by the Forwarded statistic if any such packets met this (discretionary) discard criterion.
Fragmented	Number of IPv6 packets successfully fragmented.
Fragmentation failed	Number of IPv6 packets discarded because they needed to be fragmented but could not be.
Fragments generated	Number of output packet fragments generated as a result of fragmentation.
Multicast packets	Number of multicast packets transmitted.

Release History

Release 6.6.1; command was introduced.

Related Commands

show ipv6 icmp statistics	Displays IPv6 ICMP statistics.

MIB Objects

```
ipv6IfStatsTable
   ipv6IfStatsInReceives
   ipv6IfStatsInHdrErrors
   ipv6IfStatsInTooBigErrors
   ipv6IfStatsInNoRoutes
   ipv6IfStatsInAddrErrors
   ipv6IfStatsInUnknownProtos
   ipv6IfStatsInTruncatedPkts
   ipv6IfStatsInDiscards
   ipv6IfStatsInDelivers
   ipv6IfStatsOutForwDatagrams
   ipv6IfStatsOutRequests
   ipv6IfStatsOutDiscards
   ipv6IfStatsOutFragOKs
   ipv6IfStatsOutFragFails
   ipv6IfStatsOutFragCreates
   ipv6IfStatsReasmReqds
   ipv6IfStatsReasmOKs
   ipv6IfStatsReasmFails
   ipv6IfStatsInMcastPkts
   ipv6IfStatsOutMcastPkts
```

clear ipv6 traffic

Resets all IPv6 traffic counters.

clear ipv6 traffic

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use the **show ipv6 traffic** command to view current IPv6 traffic statistics.

Examples

```
-> clear ipv6 traffic
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show ipv6 traffic	Displays IPv6 traffic statistics.

MIB Objects

```
alaIPv6ConfigTable
   alaIPv6ClearTraffic
```

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

show ipv6 tcp ports	Displays TCP Over IPv6 Connection Table.

MIB Objects

```
IPv6UdpTable
   IPv6UdpEntry
   IPv6UdpLocalAddress
   IPv6UdpLocalPort
```

```
IPv6UdpIfIndex
```

show ipv6 information

Displays IPv6 information.

show ipv6 information

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ipv6 information

Default hop limit                     = 64
Path MTU entry minimum lifetime (min) = 60
Neighbor stale lifetime (min)         = 1440
```

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.

Release History

Release 6.6.1; command was introduced.

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
```

show ipv6 ra-filter vlan

Displays the list of VLANs configured for RA filtering.

show ipv6 ra-filter vlan [*number***]**

Syntax Definitions

number	VLAN on which RA filtering is enabled.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ipv6 ra-filter vlan
vlan status
------+-------------
10 active
15 active
```

output definitions

VLAN	The VLAN on which RA filtering is enabled.
Status	Status of the VLAN.

Release History

Release 6.7.1; command introduced.

Related Commands

ipv6 ra-filter	Configures the Router Advertisement (RA) filtering on an IPv6 VLAN.

MIB Objects

```
alaIpv6RafVlanTable
   alaIpv6RafVlan
```

show ipv6 ra-filter counters

Displays the counter statistics of the NIs which are up.

show ipv6 ra-filter counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ipv6 ra-filter counters
NI     Untrusted Packet Count
----+-------------------------
1       0
```

output definitions

NI	Displays the NI in which RA filtering is enabled.
Untrusted Packet Count	Displays the dropped packets count in untrusted port.

Release History

Release 6.7.1; command introduced.

Related Commands

ipv6 ra-filter	Configures the Router Advertisement (RA) filtering on an IPv6 VLAN.

MIB Objects

```
alaIpv6RafCounterStatsTable
   alaIpv6RafNi
   alaIpv6RafUntrustedPktCnt
```

ipv6 redist

Controls the conditions for redistributing IPv6 routes between different protocols.

ipv6 redist {local | static | rip} into {rip} route-map *route-map-name* **[status {enable | disable}]**

no ipv6 redist {local | static} into {rip} [route-map *route-map-name***]**

Syntax Definitions

local	Redistributes local IPv6 routes.
static	Redistributes static IPv6 routes.
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 6450, 6350

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.
- 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 static route-map rip-to-static1
-> ipv6 redist rip into static route-map rip-to-static2
-> no ipv6 redist rip into static 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 6.6.1; command was 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 6450, 6350

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 6.6.1; command was 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 6450, 6350

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 6.6.1; command was 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]

Syntax Definitions

rip	Displays the route map redistribution configurations that specify RIP as the destination (into) protocol.

Defaults

By default all route map redistribution configurations are shown.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Examples

```
-> show ipv6 redist

Source       Destination
Protocol     Protocol     Status    Route Map
-------------+------------+---------+--------------------
localIPv6    RIPng        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 6450, 6350

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 6.6.1; command was 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 6450

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 6.6.1; command was introduced.

Related Commands

ipv6 rip status	Enables/disables RIPng routing on the switch.
show ipv6 rip	Displays RIPng status and general configuration parameters.

MIB Objects

```
alaDrcTmConfig
   alaDrcTmIPRipngStatus
```

ipv6 rip status

Enables or disables RIPng on the switch.

ipv6 rip status {enable | disable}

Syntax Definitions

N/A

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6450

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 6.6.1; command was introduced.

Related Commands

ipv6 load rip	Loads RIPng into memory.
show ipv6 rip	Displays RIPng status and general configuration parameters.

MIB Objects

```
alaProtocolripng
   alaRipngProtoStatus
```

ipv6 rip invalid-timer

Configures the amount of time a route remains active in RIB before being moved to the “Garbage” state.

ipv6 rip invalid-timer *seconds*

Syntax Definitions

seconds	Time, in seconds, that a route will remain in an “Active” state. Valid range is 1 - 300.

Defaults

parameter	default
seconds	180

Platforms Supported

OmniSwitch 6450

Usage Guidelines

This timer is reset each time a routing update is received.

Examples

```
-> ipv6 rip invalid-timer 300
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ipv6 rip garbage-timer	Configures the RIPng garbage timer value.
ipv6 rip holddown-timer	Configures the amount of time a route is placed in a holddown state.

MIB Objects

```
alaProtocolripng
   alaRipngInvalidTimer
```

ipv6 rip garbage-timer

Configures the RIPng garbage timer value. When a route in the RIB exceeds the configured Invalid Timer Value, the route is moved to a “Garbage” state in the the RIB. The garbage timer is the length of time a route will stay in this state before it is flushed from the RIB.

ipv6 rip garbage-timer *seconds*

Syntax Definitions

seconds	Time, in seconds, that a route will remain in the RIPng Routing Table before it is flushed from the RIB. Valid range is 0 - 180.

Defaults

parameter	default
seconds	120

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the **ipv6 rip invalid-timer** command to set the Invalid Timer Value.

Examples

```
-> ipv6 rip garbage-timer 180
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ipv6 rip invalid-timer	Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.
ipv6 rip holddown-timer	Configures the amount of time a route is placed in a holddown state.

MIB Objects

```
alaProtocolripng
   alaRipngGarbageTimer
```

ipv6 rip holddown-timer

Configures the amount of time a route is placed in a holddown state. Whenever a route is seen from the same gateway with a higher metric than the route in 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 6450

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 6.6.1; command was introduced.

Related Commands

ipv6 rip invalid-timer	Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.
ipv6 rip garbage-timer	Configures the RIPng garbage timer value.

MIB Objects

```
alaProtocolripng
   alaRipngHolddownTimer
```

ipv6 rip jitter

Configures an offset value for RIPng updates. This is the maximum (positive or negative) value that can be used to offset the update interval. For example, with an update interval of 30 seconds, and a jitter value of 5 seconds, the RIPng update packet would be sent somewhere (random) between 25 and 35 seconds from the previous update.

ipv6 rip jitter *value*

Syntax Definitions

value	Time, in seconds, that a routing update is offset. Valid range is 0 to one-half the updated interval value (e.g., if the updated interval is 30, the range would be 0 - 300).

Defaults

parameter	default
value	5

Platforms Supported

OmniSwitch 6450

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 6.6.1; command was introduced.

Related Commands

ipv6 rip update-interval	Configures the RIPng update interval.
show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngJitter
```

ipv6 rip route-tag

Configures the route tag value for RIP routes generated by the switch.

ipv6 rip route-tag *value*

Syntax Definitions

value	Route tag value. Valid range is 0 – 65535.

Defaults

parameter	default
value	0

Platforms Supported

OmniSwitch 6450

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 6.6.1; command was introduced.

Related Commands

show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaProtocolripng
   alaRipngRouteTag
```

ipv6 rip update-interval

Configures the RIPng update interval. This is the interval, in seconds, that RIPng routing updates will be sent out.

ipv6 rip update-interval *seconds*

Syntax Definitions

seconds	Interval, in seconds, that RIPng routing updates are sent out. Valid range is 0–120.

Defaults

parameter	default
seconds	30

Platforms Supported

OmniSwitch 6450

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 6.6.1; command was introduced.

Related Commands

ipv6 rip jitter	Configures an offset value for RIPng updates.
show ipv6 rip	Displays RIPng status and general configuration information.

MIB Objects

```
alaRipng
   alaRipngUpdateInterval
```

ipv6 rip triggered-sends

Configures the behavior of triggered updates.

ipv6 rip triggered-sends {all | updated-only | none}

Syntax Definitions

all	All RIPng routes are added to any triggered updates.
updated-only	Only route changes that are causing the triggered update are included in the update packets.
none	RIPng routes are not added to triggered updates.

Defaults

parameter	default
all | updated-only | none	**updated-only**

Platforms Supported

OmniSwitch 6450

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 6.6.1; command was 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 6450

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 25, "VLAN Management Commands".
- RIPng will support a maximum of 20 interfaces.

Examples

```
-> ipv6 rip interface Test_Lab
```

Release History

Release 6.6.1; command was 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. You can set priorities for routes generated by a switch by assigning a metric value to routes generated by that switch's RIPng interface. For example, routes generated by a neighboring switch may have a hop count of 1. However, you can lower the priority of routes generated by that switch by increasing the metric value for routes generated by the RIPng interface.

ipv6 rip interface *if_name* **metric** *value*

Syntax Definitions

if_name	IPv6 interface name.
value	Metric value. Valid range is 1 - 15.

Defaults

parameter	default
value	1

Platforms Supported

OmniSwitch 6450

Usage Guidelines

When you configure a metric for a RIPng interface, this metric cost is added to the metric of the incoming route.

Examples

```
-> ipv6 rip Test_Lab metric 1
```

Release History

Release 6.6.1; command was 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 6450

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 6.6.1; command was 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 6450

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 6.6.1; command was 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 6450

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 6.6.1; command was introduced.

Related Commands

show ipv6 rip interface	Displays information for all or specified RIPng interfaces.
show ipv6 rip routes	Displays all or a specific set of routes in the RIPng Routing Table.

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceHorizon
```

show ipv6 rip

Displays the RIPng status and general configuration parameters.

show ipv6 rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 6.6.1; command was 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 6450

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 6.6.1; command was 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 (e.g., force holddown timer).

MIB Objects

```
alaRipngInterfaceTable
   alaRipngInterfaceEntry
   alaRipngInterfaceStatus
   alaRipngInterfacePacketsRcvd
   alaRipngInterfacePacketsSent
   alaRipngInterfaceMetric
   alaRipngInterfaceIndex
   alaRipngInterfaceNextUpdate
   alaRipngInterfaceHorizon
   alaRipngInterfaceMTU
   alaRipngInterfaceSendStatus
   alaRipngInterfaceRecvStatus
```

show ipv6 rip peer

Displays a summary of the observed RIPng peers, or specific information about a peer when a peer address is provided.

show ipv6 rip peer [*ipv6_addresss*]

Syntax Definitions

ipv6_addresss	IPv6 address of the peer.

Defaults

N/A.

Platforms Supported

OmniSwitch 6450

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 6.6.1; command was introduced.

Related Commands

show ipv6 rip interface	Displays all or specified RIPng interface status.
show ipv6 rip routes	Displays all or a specific set of routes in 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 6450

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 6.6.1; command was introduced.

Related Commands

ipv6 rip interface	Creates/deletes a RIPng interface.
ipv6 rip interface metric	Configures the RIPng metric or cost for a specified interface.
show ipv6 rip interface	Displays all or specified RIPng interface status.

MIB Objects

```
alaRipngRouteTable
   alaRipngRouteEntry
   alaRipngRoutePrefixLen
   alaRipngRouteNextHop
   alaRipngRouteType
   alaRipngRouteAge
   alaRipngRouteTag
   alaRipngRouteStatus
   alaRipngRouteMetric
```

36 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 6450, 6350

Usage Guidelines

The **ip router-discovery** command only activates RDP for the switch. No advertisements occur until an IP interface is configured with RDP.

Examples

```
-> ip router-discovery enable
-> ip router-discovery disable
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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. The range is the value set for the maximum advertisement interval to 9000.

Defaults

parameter	default
seconds	3 * maximum advertisement interval

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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   Next   #Pkts
         Name          status   status    Advt sent/recvd
--------------------+--------+--------+------+---------
Marketing             Disabled  Enabled    9    0   0
Accounting            Disabled  Enabled    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**).
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,
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**).
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 6.6.1; command was introduced.

Related Commands

show ip router-discovery	Displays the current RDP status and related statistics for the entire switch.

MIB Objects

```
alaRDPIfTable
   alaRDPIfAdvtAdress
   alaRDPIfMaxAdvtInterval
   alaRDPIfMinAdvtInterval
   alaRDPIfAdvLifeTime
   alaRDPIfPrefLevel
```

37 DHCP Relay Commands

Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) packets contain configuration information for network hosts. DHCP Relay enables forwarding of BOOTP/DHCP packets between networks. This allows routing of DHCP traffic between clients and servers. It is not necessary to enable DHCP Relay if DHCP traffic is bridged through one network (clients and servers are on the same physical network).

This chapter includes a description of DHCP Relay commands that are used to define the IP address of DHCP servers, maximum number of hops, and forward delay time. Configure DHCP Relay on the switch where routing of BOOTP/DHCP packets occur.

MIB information for DHCP Relay commands is as follows:

Filename: AlcatelIND1UDPRelay.MIB
Module: ALCATEL-IND1-UDP-RELAY-MIB

A summary of the available DHCP Relay commands is listed here.

DHCP 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 trap-mode** **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-filter** **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 dhcp-snooping ip-source-filter arp-allow** **ip helper dhcp-snooping clear violation-counters** **ip helper dhcp-snooping clear global-counters** **show ip helper dhcp-snooping global-counters** **ip helper dhcp-snooping clear isf-log** **show ip helper dhcp-snooping isf-log** **ip helper boot-up enable** **ip udp relay** **ip udp relay vlan** **dhcp-server** **dhcp-server restart** **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** **clear dhcp-server statistics** **show dhcp-server leases** **show dhcp-server statistics** **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 dhcp-snooping ip-source-filter** **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** **show ipv6 helper dhcp-snooping ip-source-filter** **show ipv6 helper dhcp-snooping ip-source-filter 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 (e.g. 21.0.0.10).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Using this command enables a Global DHCP Relay service on the switch. When the DHCP Relay is specified by the DHCP server IP address, the service is called Global DHCP.
- When the DHCP Relay is specified by the VLAN number of the DHCP request, the service is referred to as Per-VLAN DHCP.
- Global DHCP and Per-VLAN DHCP are mutually exclusive. You may only configure one or the other.
- Use the **no** form of this command to delete an IP address from the DHCP Relay service. If an address is not specified, then all addresses are deleted.
- UPD Relay is automatically enabled on a switch when a DHCP server IP address is defined. There is no separate command for enabling or disabling the relay service.
- Configure DHCP Relay on switches where packets are routed between IP networks.
- You can configure up to 256 server IP addresses for one relay service.

Examples

```
-> ip helper address 75.0.0.10
-> ip helper no address 31.0.0.20
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ip helper address vlan	Specifies or deletes DHCP Relay based on the VLAN of the DHCP request.
ip helper forward delay	Sets the forward delay time value. DHCP Relay will not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
ip helper maximum hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperForwAddr
```

ip helper address vlan

Configures a DHCP Relay service for the specified VLAN. This command is used when a per-VLAN only relay service is active on the switch. It does not apply when using a standard relay service.

ip helper address *ip_address* **vlan** *vlan_id*

ip helper no address *ip_address* **vlan** *vlan_id*

Syntax Definitions

ip_address	IP address (e.g. 21.0.0.10) of the DHCP server VLAN.
vlan_id	VLAN identification number (e.g. 3) of the DHCP server VLAN.

Defaults

If no VLAN identification number is entered, VLAN ID 0 is used by default.

Platforms Supported

OmniSwitch 6450, 6350

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 (e.g., 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 vlan 3
-> ip helper no address 31.0.0.20 vlan 4
-> ip helper address 198.206.15.2 vlan 250-255
-> ip helper address 10.11.4.1 vlan 550-555 1500 1601-1620
-> ip helper no address 198.206.15.2 vlan 1601-1620
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ip helper per-vlan only	Sets the DHCP Relay forwarding option to process only DHCP packets received from a specific, identified VLAN.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperVlan
```

ip helper standard

Sets DHCP Relay forwarding option to standard. All DHCP packets are processed by a global relay service.

ip helper standard

Syntax Definitions

N/A

Defaults

By default, the DHCP Relay forwarding option is set to **standard**.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwOption
```

ip helper avlan only

Sets DHCP Relay forwarding option to process only DHCP packets received on authenticated VLAN ports.

ip helper avlan only

Syntax Definitions

N/A

Defaults

By default, the UDP forwarding option is set to **standard**.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper standard	Sets DHCP Relay forwarding option to standard. All DHCP packets are processed.
ip helper per-vlan only	Sets the DHCP Relay forwarding option to process only DHCP packets received on authenticated ports from a specific, identified VLAN.
ip helper forward delay	Sets the forward delay time value. DHCP Relay will not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
ip helper maximum hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwOption
```

ip helper per-vlan only

Sets the DHCP Relay forwarding option to process only DHCP packets received from a specific, identified VLAN. This option allows each VLAN to have its own relay.

ip helper per-vlan only

Syntax Definitions

N/A

Defaults

By default, the UDP forwarding option is set to **standard**.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper address vlan	Configures a DHCP Relay service for the specified VLAN.
ip helper standard	Sets DHCP Relay forwarding option to standard. All DHCP packets are processed.
ip helper avlan only	Sets DHCP Relay forwarding option to process only DHCP packets received on authenticated VLAN ports from clients that are not yet authenticated.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwOption
```

ip helper forward delay

Sets the forward delay time value for the DHCP Relay configuration. The BOOTP/DHCP packet the client sends contains the elapsed boot time. This is the amount of time, in seconds, since the client last booted. DHCP Relay will not process the packet unless the client's elapsed boot time value is equal to or greater than the configured value of the forward delay time.

ip helper forward delay *seconds*

Syntax Definitions

seconds	Forward delay time value in seconds (1–65535). Do not use commas in the value.

Defaults

By default, the forward delay time is set to three seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper address	Adds or deletes one or more DHCP server IP addresses to the DHCP Relay configuration.
ip helper maximum hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperForwDelay
```

ip helper maximum hops

Sets the maximum number of hops value for the DHCP Relay configuration. This value specifies the maximum number of relays a BOOTP/DHCP packet is allowed to traverse until it reaches its server destination. Limiting the number of hops that can forward a packet prevents packets from looping through the network.

ip helper maximum hops *hops*

Syntax Definitions

hops	The maximum number of relays (1–16).

Defaults

By default, the maximum hops value is set to four hops.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper address	Adds or deletes one or more DHCP server IP addresses to the DHCP Relay configuration.
ip helper forward delay	Sets the forward delay time value. DHCP Relay will not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperStatTable
   iphelperMaxHops
```

ip helper agent-information

Enables or disables the DHCP relay agent information option (Option-82) feature. When this feature is enabled, local relay agent information is inserted into client DHCP packets when the agent forwards these packets to a DHCP server.

ip helper agent-information {enable | disable}

Syntax Definitions

enable	Enables the relay agent Option-82 feature for the switch.
disable	Disables the relay agent Option-82 feature for the switch.

Defaults

By default, this feature is disabled on the switch.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper agent-information policy	Configures a policy to determine how the relay agent handles DHCP packets that already contain the Option-82 field.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperAgentInformation
```

ip helper agent-information policy

Configures a policy that determines how the DHCP relay agent will handle DHCP packets that already contain an Option-82 field.

ip helper agent-information policy {drop | keep | replace}

Syntax Definitions

drop	Drop DHCP packets that already contain an Option-82 field.
keep	Keep the existing Option-82 field information and continue to relay the DHCP packet.
replace	Replace the existing Option-82 field information with local relay agent information and continue to relay the DHCP packet.

Defaults

By default, DHCP packets that already contain an Option-82 field are dropped.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper agent-information	Enables the insertion of relay agent information Option-82 into DHCP packets.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper stats	Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

```
iphelperAgentInformationPolicy
```

ip helper 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 6450, 6350

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.

Examples

```
-> ip helper pxe-support enable
-> ip helper pxe-support disable
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
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

```
iphelperPXESupport
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 6450, 6350

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 6.6.1; command was 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 trap-mode

Globally configures the DHCP Snooping trap-mode settings for the switch.

ip helper dhcp-snooping trap-mode {default | reverse-enable | hardware | software}

Syntax Definitions

default	Default DHCP snooping functionality is followed. Only the source packets are trapped to the CPU.
reverse-enable	Disable DHCP binding entry on a trusted port. The binding table will not be built for the unicast BOOTP packets sent on the trusted ports.
hardware	The packets sent with 67/67 pair will not be trapped to the CPU during DHCP snooping.
software	The DHCP packets with 67/67 pair is trapped to the CPU in addition to 67/68 and 68/67.

Defaults

By default, the DHCP snooping trap-mode is set to default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The DHCP Snooping feature must be globally enabled for the switch to use the global mode settings.

Examples

```
-> ip helper dhcp-snooping trap-mode default
-> ip helper dhcp-snooping trap-mode reverse-enable
-> ip helper dhcp-snooping trap-mode hardware
-> ip helper dhcp-snooping trap-mode software
```

Release History

Release 6.7.1 R02; command was 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

```
iphelperDhcpSnoopingTrapStatus
```

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping option-82 data-insertion	Globally enables or disables DHCP Option-82 data insertion for DHCP packets.

MIB Objects

```
iphelperDhcpSnoopingMacAddressVerificationStatus
```

ip helper dhcp-snooping option-82 data-insertion

Globally enables or disables DHCP Option-82 data insertion for DHCP packets. When this feature is enabled, the relay agent inserts the Option-82 field into DHCP packets before forwarding them to the DHCP server.

ip helper dhcp-snooping option-82 data-insertion {enable | disable}

Syntax Definitions

enable	Enables inserting the DHCP Option-82 field into DHCP packets.
disable	Disables inserting the DHCP Option-82 field into DHCP packets.

Defaults

By default, this feature is disabled.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was 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 sub option of the Option-82 field.
ip helper dhcp-snooping	.Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping binding	Enables or disables the DHCP Snooping binding table functionality
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 in both the Circuit ID and Remote ID sub option fields of the Option-82 field.

ip helper dhcp-snooping option-82 data-insertion format [base-mac | system-name | user-string *string***]**

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.

Defaults

parameter	value
base-mac | system-name | user-string *string*	**base-mac**

Platforms Supported

OmniSwitch 6450, 6350

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 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
```

Release History

Release 6.6.1; command was 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.

MIB Objects

```
iphelperDhcpSnoopingOption82FormatType
iphelperDhcpSnoopingOption82StringValeu
```

ip helper dhcp-snooping option-82 format ascii circuit-id

Configures the type of information that is inserted into the Option-82 Circuit ID sub option. 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 | auto-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.
auto-interface-alias	The switch automatically generates the interface-alias in the following format: *SystemName_slot_port*.
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 6450, 6350

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 sub option. Each parameter provided with this command represents a different type of information.
- Configuring the Circuit ID sub option 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** 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 inserted into the Circuit ID sub option 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 auto-interface-alias delimiter |
```

Release History

Release 6.6.3; command was 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 sub option. 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 | auto-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.
auto-interface-alias	The switch automatically generates the interface-alias in the following format: *SystemName_slot_port*.
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 6450, 6350

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 sub option. Each parameter provided with this command represents a different type of information.
- Configuring the Remote ID sub option 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** 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 inserted into the Remote ID sub option 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
delimiter /
-> ip helper dhcp-snooping option-82 format ascii remote-id user-string “Bldg. B
Server” base-mac system name vlan interface-alias auto-interface-alias delimiter |
```

Release History

Release 6.6.3; command was 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 6450, 6350

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 6.6.1; command was 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping binding	Enables or disables the DHCP Snooping binding table functionality

MIB Objects

```
iphelperDhcpSnoopingVlanTable
   iphelperDhcpSnoopingVlanNumber
   iphelperDhcpSnoopingVlanMacVerificationStatus
   iphelperDhcpSnoopingVlanOpt82DataInsertionStatus
```

ip helper dhcp-snooping port

Configures the DHCP Snooping trust mode for the port. The trust mode determines if the port will accept all DHCP traffic, block all DHCP traffic, or accept only client DHCP traffic.

ip helper dhcp-snooping port *slot1/port1***[**-*port1a***] {block | client-only | trust}**

Syntax Definitions

*slot1/port1***[**-*port1a***]**	Specifies the slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (e.g. 3/1-16).
block	Blocks all DHCP traffic on the port.
client-only	Allows only DHCP client traffic on the port.
trust	Allows all DHCP traffic on the port. The port behaves as if DHCP Snooping was not enabled.

Defaults

By default, the trust mode for a port is set to **client-only** when the DHCP Snooping feature is enabled for the switch or for a VLAN.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping vlan	Enables or disables DHCP Snooping on a per-VLAN basis.

MIB Objects

```
iphelperDhcpSnoopingPortTable
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSnoopingPortTrustMode
```

ip helper dhcp-snooping 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 6450, 6350

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 6.6.3; command was introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping vlan	Enables or disables DHCP Snooping on a per-VLAN basis.

MIB Objects

```
iphelperDhcpSnoopingPortTable
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSnoopingPortTrustMode
```

ip helper dhcp-snooping 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 (e.g. 3/1 specifies port 1 on slot 3). Use a hyphen to specify a range of ports (e.g. 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper dhcp-snooping	Globally enables or disables DHCP Snooping for the switch.
ip helper dhcp-snooping vlan	Enables or disables DHCP Snooping on a per-VLAN basis.
ip helper dhcp-snooping port	Configures the DHCP Snooping trust mode for a port.
ip helper dhcp-snooping port ip-source-filter	Configures the IP source filtering status for a DHCP Snooping port.

MIB Objects

```
iphelperDhcpSnoopingPortTable
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSnoopingPortIpTrafficSuppression
```

ip helper dhcp-snooping port ip-source-filter

Configures the IP source filtering status for the port. When ip-source-filtering 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 *slot/port***[-***port1a***] ip-source-filter {enable | disable}**

Syntax Definitions

*slot/port***[-***porta***]**	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 (or 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 6450, 6350

Usage Guidelines

- This CLI is deprecated. The CLI **ip helper dhcp-snooping ip-source-filter** can be used for configuring IP source filtering.
- This CLI is supported for backward compatibility.
- 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 6.6.1; command was introduced.
Release 6.6.4: command 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 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 binding {[enable | disable] | [*mac_address* **[port** *slot/port* | **linkagg** *num***] address** *ip_address* **vlan** *vlan_id***]}**

no ip helper dhcp-snooping binding *mac_address* **[port** *slot/port* | **linkagg** *num***] 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 | *num*	The slot and port number or linkagg that receive the DHCP request.
ip_address	The IP address that the DHCP server offered to the client.
time	The IP address lease time assigned by the DHCP server.
vlan_id	The VLAN identification number (1–4094) of the VLAN to which the client belongs.

Defaults

By default, the binding table functionality is enabled when the DHCP Snooping feature is enabled for the switch or for a VLAN.

Platforms Supported

OmniSwitch 6450, 6350

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
vlan 200
-> no ip helper dhcp-snooping binding 00:2a:95:51:6c:10 port 1/15 address
17.15.3.10 vlan 200
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ip helper dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.
ip helper dhcp-snooping binding action	Synchronizes the contents of the DHCP Snooping binding table with the contents of the **dhcpBinding.db** file saved on the switch.

MIB Objects

```
iphelperDhcpSnoopingBindingStatus
iphelperDhcpSnoopingBindingTable
   iphelperDhcpSnoopingBindingMacAddress
   iphelperDhcpSnoopingBindingIfIndex
   iphelperDhcpSnoopingBindingIpAddress
   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. All the other packets will be dropped by default. This command also provides a provision to bypass the IP source filtering on specific subnets on VLAN basis.

ip helper dhcp-snooping ip-source-filter {vlan *num* **[allow** *ip_address* **mask** *subnet_mask* **| port** *slot/port* **[-***port2***] | linkagg** *num***} {enable | disable}**

Syntax Definitions

vlan *num*	The VLAN identification number (1–4094).
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.
linkagg *num*	Specifies the link aggregate identification number.
*slot/port***[-***port2***]**	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 6450, 6350

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.
- To enable or disable specific subnets on VLAN level from IP source filtering, configure the required subnets using the **"allow** *ip_address* **mask** *subnet_mask*" option. The specified subnets will be excluded from IP source filtering.
- A maximum of 16 subnets are allowed to be excluded from source filtering on OmniSwitch 6450. On OmniSwitch 6350, only 8 subnets are allowed. **show ip helper dhcp-snooping ip-source-filter vlan** displays the subnet information on which IP source filtering is excluded.

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
-> ip helper dhcp-snooping ip-source-filter vlan 4050 allow 10.55.40.4 mask
255.255.255.252 enable
```

Release History

Release 6.6.3; command was introduced.
Release 6.7.1.R02: **allow** keyword added.

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
   iphelperDhcpSourceFilterAllowSubnetTable
   iphelperDhcpSourceFilterExpIpAddress
   iphelperDhcpSourceFilterExpIpMask
   iphelperDhcpSourceFilterVlan
   iphelperDhcpSourceFilterExpIpStatus
```

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper dhcp-snooping binding	.Enables or disables the DHCP Snooping binding table functionality.
ip helper dhcp-snooping binding action	Synchronizes the contents of the DHCP Snooping binding table with the contents of the **dhcpBinding.db** file saved on the switch.

MIB Objects

```
iphelperDhcpSnoopingBindingDatabaseSyncTimeout
iphelperDhcpSnoopingBindingDatabaseLastSyncTime
```

ip helper dhcp-snooping binding action

Triggers a purge or renew action against the DHCP Snooping binding table. A purge action clears the contents of the table. A renew action populates the table with entries saved in the **dhcpBinding.db** file.

ip helper dhcp-snooping port binding action {purge | renew}

Syntax Definitions

purge	Clears all binding table entries that are maintained in switch memory.
renew	Populates the binding table with entries saved in the **dhcpBinding.db file** located in the **/flash/switch** directory on the switch.

Defaults

By default, the timeout value is set to 300 seconds.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ip helper dhcp-snooping binding	.Enables or disables the DHCP Snooping binding table functionality.
ip helper dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.

MIB Objects

```
iphelperDhcpSnoopingBindingDatabaseAction
```

ip helper 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 6450, 6350

Usage Guidelines

- With this option disabled, the entry will be removed if the MAC address is missing from the MAC address table when the database is synchronized.
- Use the **show ip 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 6.6.1; command was introduced.

Related Commands

ip helper dhcp-snooping binding	Enables or disables the DHCP Snooping binding table functionality.
ip helper dhcp-snooping binding timeout	Configures the amount of time between each automatic save of the binding table contents to a file on the switch.

MIB Objects

```
iphelperDhcpSnoopingBindingPersistencyStatus
```

ip helper dhcp-snooping ip-source-filter arp-allow

Enabling the arp-allow function the ARP packets are not checked against the binding entries and are allowed to pass through transparently.

ip helper dhcp-snooping ip-source-filter arp-allow {enable | disable}

Syntax Definitions

enable	ARP packet are not checked against the binding entries and are allowed to pass through transparently.
disable	ARP packet are checked against the binding entries and are allowed to pass through only if a valid binding entry is found.

Defaults

By default, DHCP Snooping ip-source-filter arp-allow is disabled.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Enable this function to process the ARP packets transparently without being checked for the binding entry.
- DHCP Snooping and ISF must be enabled before enabling this command.
- Use the **show ip helper** command to display the current status.

Examples

```
-> ip helper dhcp-snooping ip-source-filter arp-allow enable
-> ip helper dhcp-snooping ip-source-filter arp-allow disable
```

Release History

Release 6.7.1 R03; command was introduced.

Related Commands

show ip helper	Displays the current DHCP Relay, Relay Agent Information, and DHCP Snooping configuration.

MIB Objects

```
iphelperDhcpSnoopingArpAllowStatus
```

ip helper dhcp-snooping clear violation-counters

This command clears DHCP snooping violation counters.

ip helper dhcp-snooping clear violation-counters {all | slot *num* **| linkagg** *num* | *slot/port* | *slot/port1-port2***}**

Syntax Definitions

all	Clears DHCP snooping violation counters on all ports.
num	Clears DHCP snooping violation counter for ports of the specified slot or specified linkagg.
slot/port	Clears DHCP snooping violation counter for the specified physical port.
slot/port1-port2	Clears DHCP snooping violation counter for the specified physical port range.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to clear the DHCP snooping violation counters for all the ports or for specific ports/ linkagg
- Use the **ip helper dhcp-snooping clear global-counters** command to clear DHCP global counters

Examples

```
-> ip helper dhcp-snooping clear violation-counters all
-> ip helper dhcp-snooping clear violation-counters 1/2-6
```

Release History

Release 6.7.2.R02; command was introduced.

Related Commands

ip helper dhcp-snooping clear global-counters	This command clears the global counters for DHCP snooping or DHCP Relay.

MIB Objects

N/A

ip helper dhcp-snooping clear global-counters

This command clears the global counters for DHCP snooping.

ip helper dhcp-snooping clear global-counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to clear the statistics for DHCP snooping global counters.
- Use the **ip helper dhcp-snooping clear violation-counters** command to clear DHCP snooping violation counters

Examples

```
-> ip helper dhcp-snooping clear global-counters
```

Release History

Release 6.7.2.R02; command was introduced.

Related Commands

ip helper dhcp-snooping clear violation-counters	This command clears DHCP snooping violation counters.

MIB Objects

N/A

show ip helper dhcp-snooping global-counters

Displays the DHCP snooping global counters

show ip helper dhcp-snooping global-counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to display the statistics for DHCP snooping global counters.
- Use the **ip helper dhcp-snooping clear violation-counters** command to clear DHCP snooping violation counters

Examples

```
-> show ip helper dhcp-snooping global-counters
CMM Counters:
  DHCP Discover Packets                          : 2,
  DHCP Offer Packets                             : 0,
  DHCP Request Packets                           : 0,
  DHCP ACK Packets                               : 0,
  DHCP NACK Packets                              : 0,
  DHCP Release Packets                           : 0,
  DHCP Decline Packets                           : 0,
  DHCP Inform Packets                            : 0,
  Total Packet received in CMM                   : 2,
  Binding error (TCAM Unavailable)               : 0,
  Unknown/Malformed Packets Dropped              : 0,
  Packet drop CMM to NI (Internal Error)         : 0
NI Counters:
  Total DHCP Packets received in QDispatcher     : 2,
  Packet received in NI from QDispatcher         : 2,
  Packet received in NI from CMM                 : 0,
  Packet send to QDriver from NI                 : 0,
  Total ISF Packet Drop                          : 0,
  Packet drop QDispatcher to NI (Internal Error) : 0,
  Packet drop NI to CMM (Internal Error)         : 0,
  Packet drop NI to QDriver (Internal Error)     : 0999
```

output definitions

DHCP Discover Packets	Displays the statistics of DHCP Discover packets.
DHCP Offer Packets	Displays the statistics of DHCP Offer packets. DHCP servers on a network that receive a DHCP Discover message respond with a DHCP Offer message, which offers the client an IPv4 address lease.
DHCP Request Packets	Displays the statistics of DHCP Request packets. Clients accept the first offer received by broadcasting a DHCP Request message for the offered IPv4 address.
DHCP ACK Packets	Displays the statistics of DHCP acknowledgement packets. The server accepts the request by sending the client a DHCP Acknowledgment message.
DHCP NACK Packets	Displays the statistics of DHCP NACK packets. If the IPv4 address requested by the DHCP client cannot be used (another device may be using this IPv4 address), the DHCP server responds with a DHCPNACK (Negative Acknowledgment) packet. After this, the client must begin the DHCP lease process again.
DHCP Release Packets	Displays the statistics DHCP Release packets. A DHCP client sends a DHCP Release packet to the server to release the IPv4 address and cancel any remaining lease.
DHCP Decline Packets	Displays the statistics of DHCP Decline packets. If the DHCP client determines the offered TCP/IP configuration parameters are invalid, it sends a DHCP Decline packet to the server. After this, the client must begin the DHCP lease process again.
DHCP Inform Packets	Displays the statistics of DHCPInform packets. DHCPInform is used by DHCP clients to obtain DHCP options.
Total Packet received in CMM	Displays the total packets received in the CMM.
Binding error (TCAM Unavailable)	Displays the number of binding errors.
Unknown/Malformed Packets Dropped	Displays the number of unknown or malformed IP packets dropped.
Packet drop CMM to NI (Internal Error)	Displays the packet drop from CMM to NI due to internal errors.
Total DHCP Packets received in QDispatcher	Displays the total DHCP packets received in QDispatcher.
Packet received in NI from CMM	Displays the packet received in NI from CMM.
Packet send to QDriver from NI	Displays the packets sent to QDriver from NI.
Total ISF Packet Drop	Total number of IP source filter (ISF) packets dropped.
Packet drop QDispatcher to NI (Internal Error)	Displays the packet drop QDispatcher to NI.
Packet drop NI to QDriver (Internal Error)	Displays packet drop NI to QDriver.

Release History

Release 6.7.2.R02; command was introduced.

Related Commands

ip helper dhcp-snooping clear violation-counters	This command clears DHCP snooping violation counters.
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.

MIB Objects

N/A

ip helper dhcp-snooping clear isf-log

This command clears the IP source filter (ISF) log buffer.

ip helper dhcp-snooping clear isf-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to clear the ISF log statistics.
- Use the **show ip helper dhcp-snooping isf-log** command to display DHCP snooping ISF logs.

Examples

```
-> ip helper dhcp-snooping clear isf-log
```

Release History

Release 6.7.2.R02; command was introduced.

Related Commands

show ip helper dhcp-snooping isf-log	.This command displays the IP source filter (ISF) log buffer.

MIB Objects

N/A

show ip helper dhcp-snooping isf-log

This command displays the IP source filter (ISF) log buffer.

ip helper dhcp-snooping clear isf-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to display the ISF log statistics for DHCP snooping.
- Use the **ip helper dhcp-snooping clear isf-log** command to clear DHCP snooping violation counters

Examples

```
-> show ip helper dhcp-snooping isf-log
Date     Time     Log Message
--------+--------+-------------------------------------------------------------
1/15/15 20:06:43 In qosNIMsgLogISFRule:1503: Rule ISF-DROP matched
1/15/15 20:06:43 In qosNIMsgLogISFRule:1509: Tagged. 802.1p 0
1/15/15 20:06:43 In qosNIMsgLogISFRule:1512: svlan 100 VRF (null) port 1/46
1/15/15 20:06:43 In qosNIMsgLogISFRule:1522: MAC 02:12:45:86:23:58 ->
15:32:54:00:12:23
1/15/15 20:06:43 In qosNIMsgLogISFRule:1591: TOS 0x00 (TCP) 1.0.0.3:129 ->
1.0.0.9:128
```

Release History

Release 6.7.2.R02; command was introduced.

Related Commands

ip helper dhcp-snooping clear isf-log	This command clears the IP source filter (ISF) log buffer.

MIB Objects

N/A

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 6450, 6350

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 disable9999
```

Release History

Release 6.6.1; command was introduced.
Release 6.6.2; 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 6450, 6350

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 6.6.1; command was introduced.
Release 6.6.2; command deprecated; use **ip interface dhcp-client**.

Related Commands

ip helper dhcp-snooping ip-source-filter arp-allow	Enables or disables automatic IP configuration for the switch.

MIB Objects

```
iphelperStatTable
   iphelperBootupPacketOption
```

ip udp relay

Enables or disables UDP port relay for BOOTP/DHCP and generic UDP service ports (i.e., NBNS/NBDD, other well-known UDP ports, and user-defined service ports that are not well-known).

ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port* **[***name***]}**

no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***}**

Syntax Definitions

BOOTP	BOOTP/DHCP well-known ports 67/68.
NBDD	NBDD well-known port 138.
NBNSNBDD	NBNS/NBDD well-known ports 137/138.
DNS	DNS well-known port 53.
TACACS	TACACS well-known port 65.
TFTP	TFTP well-known port 69.
NTP	NTP well-known port 123.
port	Any number that is not a well-known port number.
name	Text string description up to 30 characters.

Defaults

By default, relay is enabled on the BOOTP/DHCP well-known ports.

parameter	default
name	User Service Other#

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to disable UDP Relay for the specified service port.
- Only use the *port* parameter to specify service port numbers that are not well known. For example, do not specify port 53 as it is the well-known port number for DNS. Instead, use the **DNS** parameter to enable relay for port 53.
- The *name* parameter is only used with the *port* parameter and provides a user-defined description to identify the not well-known port service.
- When entering a *name* for a user-defined service, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the *name* “A UDP Protocol” requires quotes because of the spaces between the words.
- When UDP Relay is disabled for BOOTP/DHCP, the **ip helper** configuration is *not* retained and all dependant functionality (i.e., automatic IP configuration for VLAN 1, Telnet and HTTP client authentication, etc.) is disrupted.

- Up to three types of UDP Relay services are supported at any one time and in any combination.

Note. If the relay service for BOOTP/DHCP is disabled when the switch reboots, the service is automatically enabled when the switch comes back up. If there were three non-BOOTP/DHCP relay services already enabled before the reboot, the most recent service enabled is disabled and replaced with the BOOTP/DHCP relay service.

- If port relay is enabled for the NBDD well-known port, NBNS is not automatically enabled by default. Specify **NBNS/NBDD** to enable relay for both well-known ports.
- Note that when UDP port relay is enabled for NTP, relay cannot forward NTP packets that contain a destination IP address that matches a VLAN router IP address on the switch.

Examples

```
-> ip udp relay DNS
-> ip udp 3047 “Generic Service”
-> no ip udp relay BOOTP
-> no ip udp relay 3047
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ip udp relay vlan	Specifies the VLAN to which traffic from the specified UDP service port is forwarded.

MIB Objects

```
iphelperxServicePortAssociationTable
   iphelperxServicePortAssociationService
   iphelperxServicePortAssociationPort
   iphelperxServicePortAssociationName
iphelperxPortServiceAssociationTable
   iphelperxPortServiceAssociationService
   iphelperxPortServiceAssociationPort
   iphelperxPortServiceAssociationName
```

ip udp relay vlan

Specifies a VLAN on which traffic destined for a UDP port is forwarded.

ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***} vlan** *vlan_id*

no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port***} vlan** *vlan_id*

Syntax Definitions

BOOTP	BOOTP/DHCP well-known ports 67/68.
NBDD	NBDD well-known port 138.
NBNSNBDD	NBNS/NBDD well-known ports 137/138.
DNS	DNS well-known port 53.
TACACS	TACACS well-known port 65.
TFTP	TFTP well-known port 69.
NTP	NTP well-known port 123.
port	A user-specified port that is not a well-known port.
vlan_id	A numeric value (1–4094) that uniquely identifies an individual VLAN. Use a hyphen to specify a range of VLANs (e.g., 1-5).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove the VLAN association with the UDP service port.
- The maximum number of VLANs that can receive forwarded UDP service port traffic is 256.
- Only specify service port numbers that are *not* well known when using the *port* parameter with this command. For example, do not specify port 53 as it is the well-known port number for the DNS UDP service. Instead, use the **DNS** parameter to enable relay for port 53.
- Specifying a VLAN for the BOOTP/DHCP service does not work if the **per-vlan only** forwarding option is not active. Use the **ip helper per-vlan only** command to enable this option.

Examples

```
-> ip udp relay DNS vlan 10
-> ip udp 3047 vlan 500
-> no ip udp relay DNS vlan 10
```

Release History

Release 6.6.1; command was introduced.

Related Commands

ip udp relay	Enables or disables relay for UDP service ports.

MIB Objects

```
iphelperxPortServiceAssociationTable
   iphelperxPortServiceAssociationService
```

dhcp-server

Enables or disables the DHCP server operation.

dhcp-server {enable | disable}

Syntax Definitions

enable	Enables operation status of the DHCP server.
disable	Disables operation status of the DHCP server.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When DHCP server is enabled on the switch, DHCP relay and DHCP snooping will not be supported on the default VRF of the switch.
- DHCP server must be restarted when changes are made to the dhcpd.conf file.

Examples

```
-> dhcp-server enable
-> dhcp-server disable
```

Release History

Release 6.6.4; command was introduced.

Related Commands

show dhcp-server leases	Displays the leases offered by the DHCP server.
show dhcp-server statistics	Displays the statistics of the DHCP server.
dhcp-server restart	Allows to restart the DHCP server when the dhcpd.conf file is modified.

MIB Objects

`alaDhcpSrvGlobalConfigStatus`

dhcp-server restart

Allows to restart the DHCP server when the dhcpd.conf file is modified.

dhcp-server restart

Syntax Definitions

restart	Restarts the DHCP server.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The command can be used to restart the DHCP server when the dhcpd.conf file is modified.

Examples

```
-> dhcp-server restart
```

Release History

Release 6.6.4; command was introduced.

Related Commands

dhcp-server	Enables or disables the DHCP server operation.

MIB Objects

```
alaDhcpSrvGlobalRestart
```

show dhcp-server leases

Displays the leases offered by the DHCP server.

show dhcp-server leases [ip- address *ip_address* **| mac-address** *mac_address***] [type {static | dynamic }] [count]**

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.
count	Count of DHCP messages recorded.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

DHCP server should be enabled first before using this command.

Examples

```
-> show dhcp-server leases

Total leases: 8

IP Address MAC address        Lease Granted         Lease Expiry          Type
---------+------------------+--------------------+--------------------+-----------
200.0.1.1 00:00:01:b8:91:3f  DEC 15 14:10:59 2009  DEC 19 01:30:59 2009  DYNAMIC
200.0.1.2 00:00:01:b8:91:37  DEC 15 14:11:05 2009  DEC 19 01:31:05 2009  DYNAMIC
200.0.1.3 00:00:01:b8:91:3b  DEC 15 14:11:48 2009  DEC 19 01:31:48 2009  DYNAMIC
200.0.1.4 00:00:01:b8:91:3d  DEC 15 14:11:53 2009  DEC 19 01:31:53 2009  DYNAMIC
220.0.0.2 00:00:01:1d:4f:7e  DEC 15 14:11:45 2009  DEC 15 22:31:45 2009  DYNAMIC
220.0.0.3 00:00:01:5a:0b:76  DEC 15 14:12:00 2009  DEC 15 22:32:00 2009  DYNAMIC
220.0.0.4 00:00:01:1d:4f:7d  DEC 15 14:11:53 2009  DEC 15 22:31:53 2009  DYNAMIC
120.0.0.4 00:00:02:12:4f:8c  DEC 15 14:11:53 2009  DEC 15 23:31:53 2009  STATIC

-> show dhcp-server leases ip-address 200.0.1.2

IP Address  MAC address        Lease Granted         Lease Expiry          Type
----------+------------------+--------------------+--------------------+---------
200.0.1.2  00:00:01:b8:91:37  DEC 15 14:11:05 2009  DEC 19 01:31:05 2009  DYNAMIC
```

```
-> show dhcp-server leases mac-address 00:00:01:1d:4f:7d

IP Address MAC address        Lease Granted         Lease Expiry          Type
----------+-----------------+--------------------+---------------------+----------
220.0.0.4  00:00:01:1d:4f:7d DEC 15 14:11:53 2009  DEC 15 22:31:53 2009  DYNAMIC
-> show dhcp-server leases type static

Total leases: 1

IP Address  MAC address        Lease Granted         Lease Expiry         Type
----------+-----------------+--------------------+--------------------+-----------
120.0.0.4  00:00:02:12:4f:8c  DEC 15 14:11:53 2009 DEC 15 23:31:53 2009  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.
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 6.6.4; 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 leases related to the DHCP server.
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 6450, 6350

Usage Guidelines

DHCP server should be enabled first before using this command.

Examples

```
-> show dhcp-server statistics
General:
  DHCP Server Name: mample.vitalqip.com,
   DHCP Server Status         : Enabled,
   Total Subnets Managed      : 7,
   Total Subnets Used         : 2,
   Total Subnets Unused       : 5,
   Total Subnets Full         : 0,
   DHCP Server System Up Time : TUE DEC 15 14:10:27.9956
     Lease DB Sync:
Lease DB Sync time (in sec)  : 60,
      Last sync time        : TUE DEC 15 14:21:34 2009,
      Next sync time        : TUE DEC 15 14:22:34 2009

-> show dhcp-server statistics packets
Packets:
   Total DHCP Discovers       : 12,
   Total DHCP Offers          : 12,
   Total DHCP Requests        : 16,
   Total DHCP Request Grants  : 10,
   Total DHCP Request Renews  : 6,
   Total DHCP Declines        : 0,
   Total DHCP Acks            : 16,
```

```
  Total DHCP Nacks           : 0,
  Total DHCP Releases        : 0,
  Total DHCP Informs         : 0,
  Total Bootp requests       : 0,
  Total Bootp response       : 0,
  Total Unknown packets      : 0

-> show dhcp-server statistics hosts
Leases:
    Total:
      Leases Managed: 1365,
      Leases used              : 7,
      Leases unused            : 1358,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Static DHCP:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Dynamic DHCP:
      Leases Managed           : 1365,
      Leases used              : 7,
      Leases unused            : 1358,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Automatic DHCP:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Static Bootp:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Automatic Bootp           :
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0

-> show dhcp-server statistics subnets
Subnets:
    Subnet1:
      Subnet: 200.0.0.0,
      Total                    : 1022,
      Static DHCP              : 0,
      Dynamic DHCP             : 1022,
      Automatic DHCP           : 0,
      Static Bootp             : 0,
      Automatic Bootp          : 0
        Ranges:
          Start                : 200.0.1.1,
          End                 : 200.0.2.255,
```

```
            Mask                : 255.255.253.0,
            Type                : 5
            Used                : 4,
            Unused              : 507,
            Pending             : 0,
            Unavailable         : 0
      Subnet2:
        Subnet                  : 220.0.0.0,
        Total                    : 508,
        Static DHCP              : 0,
        Dynamic DHCP             : 508,
        Automatic DHCP           : 0,
        Static Bootp             : 0,
        Automatic Bootp          : 0
          Ranges:
         Start                  : 220.0.0.2,
         End                    : 220.0.0.255,
         Mask                   : 255.255.255.0,
         Type                   : 5,
         Unused                 : 251,
         Used                   : 3,
         Pending                : 0,
         Unavailable            : 0
      Subnet3:
        Subnet                  : 150.0.0.0,
        Total                    : 400,
        Static DHCP              : 0,
        Dynamic DHCP             : 400,
        Automatic DHCP           : 0,
        Static Bootp             : 0,
        Automatic Bootp          : 0
          Ranges:
            Range1:
              Start             : 150.0.1.1,
              End               : 150.0.1.100,
             Mask               : 255.255.255.0,
              Type              : 5,
              Used              : 0,
              Unused             : 100,
              Pending            : 0,
              Unavailable        : 0
            Range2:
              Start             : 150.0.2.1,
              End               : 150.0.2.100,
              Mask              : 255.255.255.0,
              Type              : 5,
              Unused             : 100,
              Used              : 0,
              Pending            : 0,
              Unavailable        : 0
    Subnet4:
        Subnet                  : 50.0.0.0,
        Total                   : 200,
        Static DHCP              : 0,
        Dynamic DHCP             : 200,
        Automatic DHCP          : 0,
        Static Bootp             : 0,
        Automatic Bootp         : 0
          Ranges:
```

```
           Start              : 50.0.1.1,
           End                : 50.0.1.100,
           Mask               : 255.255.255.0,
           Type               : 5,
           Unused             : 100,
           Used               : 0,
           Pending            : 0,
           Unavailable        : 0

-> show dhcp-server statistics all
General:
  DHCP Server Name: mample.vitalqip.com,
  DHCP Server Status         : Enabled,
  Total Subnets Managed      : 7,
  Total Subnets Used         : 2,
  Total Subnets Unused       : 5,
  Total Subnets Full         : 0,
  DHCP Server System Up Time : TUE DEC 15 14:10:27.9956
    Lease DB Sync:
      DB Sync time (in sec)   : 60,
      Last sync time          : TUE DEC 15 14:21:34 2009,
      Next sync time          : TUE DEC 15 14:22:34 2009
Packets:
  Total DHCP Discovers: 12,
  Total DHCP Offers          : 12,
  Total DHCP Requests        : 16,
  Total DHCP Request Grants  : 10,
  Total DHCP Request Renews  : 6,
  Total DHCP Declines        : 0,
  Total DHCP Acks            : 16,
  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:
    Total:
      Leases Managed: 1365,
      Leases used              : 7,
      Leases unused            : 1358,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Static DHCP:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Dynamic DHCP:
      Leases Managed           : 1365,
      Leases used              : 7,
      Leases unused            : 1358,
      Leases Pending           : 0,
      Leases unavailable       : 0
    Automatic DHCP:
      Leases Managed           : 0,
      Leases used              : 0,
      Leases unused            : 0,
```

```
        Leases Pending           : 0,
        Leases unavailable       : 0
      Static Bootp:
        Leases Managed           : 0,
        Leases used              : 0,
        Leases unused            : 0,
        Leases Pending           : 0,
        Leases unavailable       : 0
      Automatic Bootp           :
        Leases Managed           : 0,
        Leases used              : 0,
        Leases unused            : 0,
        Leases Pending           : 0,
        Leases unavailable       : 0
  Subnets:
      Subnet1:
        Subnet                  : 200.0.0.0,
        Total                    : 1022,
        Static DHCP              : 0,
        Dynamic DHCP             : 1022,
        Automatic DHCP           : 0,
        Static Bootp            : 0,
        Automatic Bootp          : 0
          Ranges:
            Start               : 200.0.1.1,
            End                 : 200.0.2.255,
            Mask                : 255.255.253.0,
            Type                : 5
            Used                : 4,
            Unused              : 507,
            Pending             : 0,
            Unavailable         : 0
      Subnet2:
        Subnet                   : 220.0.0.0,
        Total                    : 508,
        Static DHCP              : 0,
        Dynamic DHCP             : 508,
        Automatic DHCP           : 0,
        Static Bootp             : 0,
        Automatic Bootp          : 0
          Ranges:
            Start               : 220.0.0.2,
            End                 : 220.0.0.255,
            Mask                : 255.255.255.0,
            Type                : 5
           Unused               : 251,
           Used                 : 3,
           Pending              : 0,
          Unavailable           : 0
      Subnet3:
        Subnet                   : 150.0.0.0,
        Total                    : 400,
        Static DHCP              : 0,
        Dynamic DHCP             : 400,
        Automatic DHCP           : 0,
        Static Bootp             : 0,
        Automatic Bootp          : 0
          Ranges:
            Range1:
```

```
            Start             : 150.0.1.1,
            End               : 150.0.1.100,
             Mask             : 255.255.255.0,
            Type              : 5,
            Used              : 0,
            Unused            : 100,
            Pending           : 0,
            Unavailable       : 0
          Range2:
            Start             : 150.0.2.1,
            End               : 150.0.2.100,
            Mask              : 255.255.255.0,
            Type              : 5,
            Unused            : 100,
            Used              : 0,
            Pending           : 0,
            Unavailable       : 0
Subnet4:
     Subnet                   : 50.0.0.0,
     Total                    : 200,
     Static DHCP              : 0,
     Dynamic DHCP             : 200,
     Automatic DHCP           : 0,
     Static Bootp             : 0,
     Automatic Bootp          : 0
       Ranges:
         Start                : 50.0.1.1,
         End                  : 50.0.1.100,
         Mask                 : 255.255.255.0,
         Type                 : 5,
         Unused               : 100,
         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 where all 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 occurred.
Next sync time	Specifies the next time the synchronization should be scheduled.
Packet stats	Denotes statistical information about the data packet transmission.

output definitions (continued)

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.
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 acknowledgement 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 statistical 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 statistical information about the hosts configured with Static DHCP.
Automatic DHCP	Denotes statistical information about the hosts configured with Automatic DHCP.

output definitions (continued)

Static BootP	Denotes statistical information about the hosts configured under Static BootP. **Note:** BootP Relay is disabled when DHCP server is enabled on the switch.
Automatic BootP	Denotes statistical information about the hosts configured with Automatic BootP.
Subnet statistics	Denotes all DHCP related statistical information for individual subnets.
Range	Specifies the range of IP addresses in the individual subnet.
Mask	Specifies the subnet mask.
Type	Specifies whether the type of IP address allocation is dynamic or Static.

Release History

Release 6.6.4; command introduced.

Related Commands

clear dhcp-server statistics	Clears the DHCP Server lease statistics.

MIB Objects

N/A

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 6450, 6350

Usage Guidelines

Use this command to clear the packet counters of DHCP server statistics.

Examples

```
-> clear dhcp-server statistics
```

Release History

Release 6.6.4; command introduced.

Related Commands

show dhcp-server statistics	Displays the DHCP Server lease statistics.

MIB Objects

N/A

show ip helper

Displays the current DHCP Relay, Relay Agent Information, and DHCP Snooping configuration.

show ip helper

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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) = 0,
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 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 Field3 = Interface,
DHCP Snooping Opt82 ASCII Circuit ID Field3 String = - ,
DHCP Snooping Opt82 ASCII Circuit ID Field4 = Interface Alias,
DHCP Snooping Opt82 ASCII Circuit ID Field4 String = - ,
DHCP Snooping Opt82 ASCII Circuit ID Field5 = System Name,
DHCP Snooping Opt82 ASCII Circuit ID Field5 String = vxTarget,
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 Field3 = User String,
DHCP Snooping Opt82 ASCII Remote ID Field3 String = biswajit,
DHCP Snooping Opt82 ASCII Remote ID Delimiter = " ",
DHCP Snooping Trap-Mode     =  default,
```

```
DHCP Snooping Binding DB Status = Enabled,
ARP-Allow Status                = Enabled,
Database Sync Timeout = 300,
Database Last Sync Time = ,
Binding Persistency Status = Disabled,
PXE support = Disabled,
Forward option = standard
Vlan Number NA
Bootup Option Disable
Forwarding Address :
20.0.0.151
UDP Relay on Default VRF = Enabled
```

The following example shows what the display output looks like when the DHCP relay agent information (Option 82) feature is enabled and the DHCP Snooping feature is disabled:

```
-> show ip helper
Ip helper :
  Forward Delay(seconds) = 3,
  Max number of hops     = 4,
  Relay Agent Information            =  Enabled,
  Relay Agent Information Policy     =  Drop
  DHCP Snooping Status               =  Disabled
  DHCP Snooping Bypass Opt82-Check   =  Disabled,
  DHCP Snooping Opt82 Format  =  Base MAC,
  DHCP Snooping Opt82 String  =  00:d0:95:ae:3b:f6,
  DHCP Snooping Trap-Mode     =  default,
  DHCP Snooping Binding DB Status    =  Disabled,
  ARP-Allow Status                   =  Disabled,
  Forward option     = standard
      Vlan Number NA
  Bootup Option Disable
      Forwarding Address :
        5.5.5.5
        21.2.2.10
        172.19.4.1
```

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**. Configured through the **ip helper standard** command.
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 trap-mode** 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 bypass option-82-check** command.
DHCP Snooping Opt 82 Format	The type of information (base MAC address for the switch, system name for the switch, or user-defined text) that is inserted into the Option-82 field 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 Trap-Mode	Displays the configured DHCP Snooping global mode setting.
DHCP Binding DB Status	Indicates if the DHCP snooping binding table (database) functionality is **Enabled** or **Disabled**.
ARP-Allow Status	Displays the ARP-allow status for IP source filtering packets.
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.

output definitions

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 dhcp-snooping ip-source-filter arp-allow** 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 6.6.1; command was introduced.
Release 6.7.1 R02; **DHCP Snooping Trap-Mode** output field was introduced.
Release 6.7.1 R03; **ARP-Allow Status** output filed was introduced.

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.
ip helper dhcp-snooping trap-mode	Globally configures the DHCP Snooping trap-mode settings for the switch.
ip helper dhcp-snooping ip-source-filter arp-allow	Enabling the arp-allow function the ARP packets are not checked against the binding entries and are allowed to pass through transparently.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperForwAddr
   iphelperForwDelay
   iphelperMaxHops
```

```
iphelperAgentInformation
iphelperAgentInformationPolicy
iphelperDhcpSnooping
iphelperDhcpSnoopingOpt82DataInsertionStatus
iphelperDhcpSnoopingMacAddressVerificationStatus
iphelperDHCPSnoopingBypassOpt82CheckStatus
iphelperDhcpSnoopingOption82FormatType
iphelperDhcpSnoopingOption82StringValue
iphelperDhcpSnoopingBindingStatus
iphelperDhcpSnoopingTrapStatus
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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.

MIB Objects

```
iphelperStatTable
   iphelperServerAddress
   iphelperRxFromClient
   iphelperTxToServer
   iphelperMaxHopsViolation
   iphelperForwDelayViolation
   iphelperResetAll
```

show ip helper dhcp-snooping vlan

Displays a list of VLANs that have DHCP Snooping enabled and whether or not MAC address verification and Option-82 data insertion is enabled for each VLAN.

show ip helper dhcp-snooping vlan

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
show ip helper dhcp-snooping port	Displays the trust mode and DHCP violation statistics for all switch ports that are filtered by DHCP Snooping.

MIB Objects

```
iphelperDhcpSnoopingVlanTable
   iphelperDhcpSnoopingVlanNumber
   iphelperDhcpSnoopingVlanMacVerificationStatus
   iphelperDhcpSnoopingVlanOpt82DataInsertionStatus
```

show ip helper dhcp-snooping port

Displays the trust mode and DHCP Snooping violation statistics for all switch ports that are filtered by DHCP Snooping.

show ip helper dhcp-snooping port

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If DHCP Snooping is operating at the switch level, then information for all switch ports is displayed.
- If DHCP Snooping is operating at the VLAN level, then information for only those ports that are associated with a DHCP Snooping VLAN is displayed.
- The violation statistics displayed only apply to ports that are in the client only trust mode. When the trust mode for a port is changed from **client-only** to **trusted** or **blocked**, the violation counters are set to zero (0).

Examples

```
-> show ip helper dhcp-snooping port
Slot      Trust       Opt82       MAC       Server     Relay    Binding
Port      Mode      Violation  Violation  Violation  Violation Violation
-----+-------------+----------+----------+----------+----------+---------
1/1        Blocked       0          0          0          0        0
1/2    Client-Only       0          0          0          0        0
1/3    Client-Only       0          0          0          0        0
1/4    Client-Only       0          0          0          0        0
1/5    Client-Only       0          0          0          0        0
1/6        Blocked       0          0          0          0        0
1/7    Client-Only       0          0          0          0        0
1/8    Client-Only       0          0          0          0        0
1/9    Client-Only       0          0          0          0        0
1/10       Trusted       0          0          0          0        0
1/11       Trusted       0          0          0          0        0
1/12       Trusted       0          0          0          0        0
```

output definitions

Slot/Port	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
Trust Mode	The DHCP Snooping trust mode for the port (**Blocked**, **Client-Only**, or **Trusted**). Configured through the **ip helper dhcp-snooping port** command.
Opt82 Violation	The number of DHCP packets dropped due to a DHCP Snooping Option-82 violation.
MAC Violation	The number of DHCP packets dropped due to a mismatch between the packet source MAC address and the client hardware address contained within the packet.
Server Violation	The number of DHCP server packets dropped because they originated from outside the network or firewall.
Relay Violation	The number of DHCP packets dropped because the packet included a relay agent IP address that was not 0.0.0.0.
Binding Violation	The number of DHCP packets dropped due to a mismatch between packets received and binding table information.

Release History

Release 6.6.1; command was introduced.

Related Commands

show ip helper	Displays current DHCP Relay configuration information.
show ip helper dhcp-snooping vlan	Displays a list of DHCP Snooping VLANs.

MIB Objects

```
iphelperDhcpSnoopingPortTable
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSnoopingPortTrustMode
   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 [port | ipaddress | linkagg]

Syntax Definitions

port	Displays the DHCP binding table entries based on port.
ipaddress	Displays the DHCP binding table entries based on IP address.
linkagg	Displays the DHCP binding table entries based on Linkagg.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **ip helper dhcp-snooping binding** command to create a static entry in the binding table.
- Dynamic binding table entries are created when the relay agent receives a DHCPACK packet.

Examples

```
-> show ip helper dhcp-snooping binding
       MAC           Slot        IP          Lease     VLAN     Binding
     Address         Port      Address       Time<min> 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
00:12:3f:a6:a6:61    3/11   172.37.1.218     9         280     Dynamic
00:21:a0:2d:ef:64    3/11   172.37.1.214     10        280     Dynamic

-> show ip helper dhcp-snooping binding port 1/4
  Slot  MAC                 IP           Lease     VLAN     Binding
  Port  Address             Address      Time<min>  ID       Type
------+------------------+--------------+----------+-------+-----------
1/4    00:ae:22:e4:00:08  10.255.11.26     2000      5       Dynamic

-> show ip helper dhcp-snooping binding ip-address 10.255.11.23
       MAC           Slot        IP          Lease     VLAN     Binding
     Address         Port      Address       Time<min> ID       Type
------------------+------+--------------+-----------+-------+-----------
00:ae:22:e4:32:08    1/2    10.255.11.23     200       4       Dynamic

-> show ip helper dhcp-snooping binding linkagg 4
  Slot  MAC                 IP           Lease     VLAN     Binding
  Port  Address             Address      Time<min>  ID       Type
------+------------------+--------------+----------+-------+-----------
0/4    00:fe:22:e4:a6:08  10.255.11.24     2000      5       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.
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 binding** command.

Release History

Release 6.6.1; command was introduced.
Release 6.7.2.R04; **port**, **ipaddress** and **linkagg** parameter added. Output modified to display in ascending order of port number followed by linkagg in ascending order.

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 6450, 6350

Usage Guidelines

- Enter a service name or port number with this command to display information about an individual service.
- When specifying a port number, do not specify a well-known port number. Instead, use the service name for the well-known port (i.e., NBNS/NBDD, DNS, etc.).

Examples

```
-> show ip udp relay service

Service    Port(s)  Description
---------+--------+------------------
  1        67  68   BOOTP/DHCP
  4        53       DNS
  5        65       TACACS

-> show ip udp relay service dns

Service    Port(s)  Description
---------+--------+------------------
   4       53       DNS
```

```
-> show ip udp relay service 1776

Service    Port(s)  Description
---------+--------+------------------
   9       1776     A UDP protocol
```

output definitions

Service	The UDP service number. (**1** through **7** for well-known service ports and **8** and above for user-defined service ports).
Port(s)	The UDP service port number.
Description	A description of the UDP service.

Release History

Release 6.6.1; command was introduced.

Related Commands

show ip udp relay statistics	Displays the current statistics for each UDP port relay service.
show ip helper dhcp-snooping ip-source-filter	Displays the ports or VLANs on which IP source filtering is enabled or the binding table for IP source filtering enabled ports.

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 6450, 6350

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 (that is, NBNS/NBDD, DNS, and so on).

Examples

```
-> show ip udp relay statistics

Service                     Vlan    Pkts Sent   Pkts Recvd
------------------------+--------+------------+-----------
5:TACACS                                            20
                            33          20
                            34           0
6:TFTP                                              20
                            33          20
                            34           0
7:NTP                                               20
                            33          20
                            34           0
```

```
-> show ip udp relay statistics tacacs

Service                     Vlan    Pkts Sent   Pkts Recvd
------------------------+--------+-----------+-----------
5:TACACS                                            20
                            33         20
                            34          0
```

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. The packets sent count are based on the forwarding VLAN on which it is sent.
Pkts Recvd	The number of packets received by this service port from a client. The packets received are based on the service.

Release History

Release 6.6.1; command was introduced.

Related Commands

show ip udp relay service	Displays current configuration for UDP services by service name or by service port number.
show ip helper dhcp-snooping ip-source-filter	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 6450, 6350

Usage Guidelines

- Enter a service name or port number with this command to display information about an individual service.
- When specifying a port number, do not specify a well-known port number. Instead, use the service name for the well-known port (i.e., NBNS/NBDD, DNS, etc.).

Examples

```
-> show ip udp relay destination

Service          Port     VLANs
---------------+--------+----------------
BOOTP            67
DNS              53       2  4
TACACS           65       3

-> show ip udp relay destination dns

Service          Port     VLANs
---------------+--------+----------------
DNS              53       2  4
-> show ip udp relay destination 1776
```

```
Service            Port     VLANs
-----------------+--------+----------------
A UDP Protocol     1776     18
```

output definitions

Service	The active UDP service name.
Port	The UDP service port number.
VLANs	The VLAN assigned to the UDP service port that will forward traffic destined for that port. Use the **ip udp relay vlan** command to configure this value.

Release History

Release 6.1; command was introduced.

Related Commands

show ip udp relay service	Displays current configuration for UDP services by service name or by service port number.
show ip udp relay statistics	Displays the current statistics for each UDP port relay service.

MIB Objects

```
iphelperTable
   iphelperService
   iphelperVlan
iphelperxPropertiesTable
   iphelperxPropertiesName
   iphelperxPropertiesPort
```

show ip helper dhcp-snooping ip-source-filter

Displays the ports or VLANs on which IP source filtering is enabled or the binding table entries for IP source filtering enabled ports and VLANs.

show ip helper dhcp-snooping ip-source-filter {vlan | port | binding}

Syntax Definitions

vlan	Displays the VLANs on which the IP source filtering is enabled.
port	Displays the ports on which IP source filtering is enabled.
binding	Displays the binding table entries for the ports and VLANs on which the IP source filtering is enabled.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 the IP source filtering status. **Enabled** or **Disabled**.

```
-> show ip helper dhcp-snooping ip-source-filter vlan
VLAN     Ip Src      Excluded        Subnets
ID      Filtering     IP              Mask
------+------------+---------------+-------------
101     Enabled     10.55.40.4      255.255.255.252
```

output definitions

VLAN ID	Specifies the VLAN ID of the instance.
IP Src Filtering	Specifies the IP source filtering status. **Enabled** or **Disabled**.
Excluded IP	Specifies the excluded IP address on which the DHCP snooping IP source filtering exception is applied.
Subnets Mask	Specifies the subnet IP address on which the DHCP snooping IP source filtering exception is applied

```
-> show ip helper dhcp-snooping ip-source-filter binding

   MAC             Slot     IP         Lease   VLAN    Binding
 Address           Port   Address      Time     ID      Type
-----------------+------+------------+-----+------+--------------------
00:00:13:02:78:77 1/30   110.11.1.135  15     161    Dynamic

Total number of binding entries  :1
```

output definitions

MAC Address	Specifies the MAC address of allowed streams.
Slot/Port	Specifies the slot and port number on which source filtering has been enabled.
IP Address	Specifies the IP address of allowed streams.
Lease Time	Specifies the lease time of the binding entries expiry.
VLAN ID	Specifies the VLAN ID for the instance.
Binding Type	Specifies the type of binding.

Release History

Release 6.6.3; command was introduced.
Release 6.7.1 R02; **binding** parameter added.

Related Commands

ip helper dhcp-snooping binding	Enables or disables the IP source filtering at a port, link aggregation, or VLAN level.
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.

MIB Objects

```
iphelperDhcpSnoopingPortIpSourceFiltering
   iphelperDhcpSnoopingPortIfIndex
   iphelperDhcpSourceFilterVlanNumber
   iphelperDhcpSourceFilterVlanFilteringStatus
iphelperDhcpSnoopingBindingTable
   iphelperDhcpSnoopingBindingMacAddress
   iphelperDhcpSnoopingBindingIfIndex
```

```
iphelperDhcpSnoopingBindingIpAddress
iphelperDhcpSnoopingBindingVlan
iphelperDhcpSnoopingBindingLeaseTime
iphelperDhcpSnoopingBindingType
```

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 6450, 6350

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 both 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 6.7.1; command introduced.

Related Commands

ipv6 helper per-vlan only	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 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

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.7.1; 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 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 6450, 6350

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 6.7.1; 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 6450, 6350

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 6.7.1; command introduced.

Related Commands

ipv6 helper per-vlan only	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 maximum hops

Sets the maximum number of hops for the DHCPv6 Relay configuration.

ipv6 helper maximum hops *num*

Syntax Definitions

num	Maximum number of hops. The valid range is 1 to 32.

Defaults

By default, the maximum number of hops is set to 32.

Platforms Supported

OmniSwitch 6450, 6350

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 6.7.1; 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 6450, 6350

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 6.7.1; 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 6450, 6350

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 6.7.1; 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 6.7.1; 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 6.7.1; 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; 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 6.7.1; 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 6.7.1; 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 6.7.1; 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 6.7.1; 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 dhcp-snooping ip-source-filter

Enables or disables the IPv6 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 IPv6 address, MAC address, port, and VLAN combination obtained from the DHCPv6 snooping binding table entry.

ipv6 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.
*slot/port***[-***port2***]**	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, IPv6 source filtering is disabled for a port or link aggregate, or VLAN.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- In case of OmniSwitch 6350, source filtering for both IPv4 and IPv6 cannot be configured on the same switch.
- DHCPv6 snooping must be enabled for IPv6 source filtering to be enabled.
- IPv6 source filtering can be enabled
  - On the port or VLAN level when DHCPv6 snooping is enabled at the system level or VLAN level.
  - On the ports that are associated with a VLAN on which DHCPv6 snooping is enabled.
  - On all the ports or link aggregate when DHCPv6 snooping is enabled at the system level.
- When the IPv6 source filtering is enabled on the switch, only two UNI profiles can be configured.
- A maximum of 32 VLANs can be tagged to IPv6 source filtering.

Examples

```
-> ipv6 helper dhcp-snooping ip-source-filter port 1/1 enable
-> ipv6 helper dhcp-snooping ip-source-filter linkagg 2 enable
-> ipv6 helper dhcp-snooping ip-source-filter vlan 10 enable
-> ipv6 helper dhcp-snooping ip-source-filter vlan 20 disable
```

Release History

Release 6.7.1; command introduced.

Related Commands

show ipv6 helper dhcp-snooping ip-source-filter	Displays the ports or VLANs on which IPv6 source filtering is enabled.
show ipv6 helper dhcp-snooping ip-source-filter binding	Displays the binding entries for IPv6 source filtering.

MIB Objects

```
ipv6helperDhcpSnoopingPortTable
   ipv6helperDhcpSnoopingPortIfIndex
   Ipv6helperDhcpSourceFilterPortFilteringStatus
   ipv6helperDhcpSourceFilterVlanNumber
   ipv6helperDhcpSourceFilterVlanFilteringStatus
```

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 up to 255 characters.

Defaults

By default, **interface-id** option is added with value containing VLAN 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 6.7.1; 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 sub option. 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 6450, 6350

Usage Guidelines

- Configuring the Remote ID sub option 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 6.7.1; 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 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
Dhcpv6 helper :
  Max number of hops     = 32,
  DHCPV6 Snooping Status              =  VLAN-Level Enabled,
  DHCPV6 Remote-id                    =  Enabled,
  DHCPV6 Remote-id Enterprise Number  =  -,
  DHCPV6 Remote-Id Format             =  System Name,
  DHCPV6 Remote-Id  String            =  vxTarget,
  DHCPV6 Interface-id  Prefix         =  -,
  DHCPV6 Snooping Binding DB Status   =  Enabled,
  Database Sync Timeout               =  300,
  Database Last Sync Time             =  Jun  1 2015 15:17,
  Binding Persistency Status          =  Disabled,
  Forward option                      = per-vlan only

Forwarding Address                            Vlan Number
----------------------------------------------+----------------
2001:1:2000::4                                2002
```

output definitions

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 Remote-id	Specifies if remote ID is enabled or disabled.
DHCPV6 Remote-id Enterprise Number	Specifies the registered enterprise number of the vendor.
DHCPV6 Remote-Id Format	Specifies the remote ID format set.
DHCPV6 Remote-Id String	Specifies the remote ID value.
DHCPV6 Interface-id Prefix	A user-defined text string up to 255 characters.
DHCPv6 Snooping Binding DB Status	Specifies DHCPv6 Snooping Binding DB Status **Enabled,** or **Disabled**

output definitions

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 time 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**
Forwarding Address	Specifies the assigned Forwarding Address
Vlan Number	Specifies the assigned VLAN Numbers in **per-vlan only** mode.

Release History

Release 6.7.1; 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 per-vlan only	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
   ipv6helperVlan
   ipv6helperStatus
```

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 6.7.1; command introduced.

Related Commands

ipv6 helper address	Displays the DHCPv6 Relay statistics.
ipv6 helper per-vlan only	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

```
ipv6helperStatTable
   ipv6helperStatsServerAddress
   ipv6helperStatsVlan
   ipv6helperTxToServer
```

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 6.7.1; 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 6.7.1; 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

```
ipv6helperDhcpSnoopingPortTable
   ipv6helperDhcpSnoopingPortIfIndex
   ipv6helperDhcpSnoopingPortTrustMode
   ipv6helperSnoopingClientViolation
   ipv6helperSnoopingServerViolation
   ipv6helperSnoopingBindingViolation
   ipv6helperSnoopingInterfaceidViolation
   ipv6helperSnoopingPortSourceFilterStatus
```

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
```

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.
VLAN ID	Specifies the VLAN IDs on which DHCPv6 snooping binding is active.

Release History

Release 6.7.1; 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
   ipv6helperBindingLinkLocalAddress
   ipv6helperBindingVlan
   ipv6helperBindingIfIndex
   ipv6helperBindingGlobalIpv6Address
   ipv6helperBindingLeaseTime
   ipv6helperBindingRowStatus
```

show ipv6 helper dhcp-snooping ip-source-filter

Displays the ports or VLANs on which IPv6 source filtering is enabled.

show ip helper dhcp-snooping ip-source-filter {port | vlan}

Syntax Definitions

port	Displays the ports on which IPv6 source filtering is enabled.
vlan	Displays the VLANS on which IPv6 source filtering is enabled.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The show output displays only those ports and VLANs on which IPv6 source filtering is enabled.
- This command also displays the status of the link aggregate ports, when source filtering is enabled at port level.

Examples

```
-> show ipv6 helper dhcp-snooping ip-source-filter port
Slot    IPV6 Src
Port   Filtering
------+------------
1/9     Enabled

-> show ipv6 helper dhcp-snooping ip-source-filter vlan
 VLAN    IpV6 Src
  ID    Filtering
------+------------
 2002    Enabled
```

output definitions

Slot/Port	Specifies the slot and port number.
VLAN ID	The VLAN ID.
IPv6 Src Filtering	Specifies the IPv6 source filtering status. **Enabled** or **Disabled**.

Release History

Release 6.7.1; command introduced.

Related Commands

ipv6 helper dhcp-snooping ip-source-filter	Enables or disables the IPv6 source filtering capability at a port, link aggregation, or VLAN level.

MIB Objects

```
ipv6helperSourceFilterVlanTable
   ipv6helperSourceFilterVlan
ipv6helperDhcpSnoopingPortTable
   ipv6helperDhcpSnoopingPortIfIndex
   ipv6helperDhcpSnoopingPortTrustMode
   ipv6helperSnoopingClientViolation
   ipv6helperSnoopingServerViolation
   ipv6helperSnoopingBindingViolation
   ipv6helperSnoopingInterfaceidViolation
   ipv6helperSnoopingPortSourceFilterStatus
```

show ipv6 helper dhcp-snooping ip-source-filter binding

Displays the binding entries for IPv6 source filtering.

show ip helper dhcp-snooping ip-source-filter binding

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ipv6 helper dhcp-snooping ip-source-filter 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
```

output definitions

Link-local Address	Specifies the IPv6 address configured for the IP source filter binding.
Slot/Port	Specifies the slot and port number.
IPv6 Address	IPv6 address.
Valid LifeTime	Specifies the valid binding lease life time.
VLAN ID	The VLAN Id.

Release History

Release 6.7.1; command introduced.

Related Commands

ipv6 helper dhcp-snooping ip-source-filter	Enables or disables the IPv6 source filtering capability at a port, link aggregation, or VLAN level.

MIB Objects

N/A

38 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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
```

39 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 25, "VLAN Management Commands".

Examples

```
-> ip rip interface rip-1
```

Release History

Release 6.6.1; 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 6450

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 25, “VLAN Management Commands”.

Examples

```
-> ip rip interface rip-1 status enable
```

Release History

Release 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

Usage Guidelines

Only RIPv2 supports route tags.

Examples

```
-> ip rip route-tag 0
```

Release History

Release 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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 6450

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 6.6.1; 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
   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 6450

Usage Guidelines

The invalid time interval value must be three times the update interval value.

Examples

```
-> ip rip invalid-timer 270
```

Release History

Release 6.6.1; 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
   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 6450

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 6.6.1; 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
   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 6450

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 6.6.1; 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
   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 6450

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 6.6.1; command was introduced.

Related Commands

ip rip status	Enables/disables RIP routing on the switch.
ip rip force-holddowntimer	Configures the interval during which a RIP route remains in 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 6450

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 6.6.1; command was introduced.

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 6450

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 6.6.1; 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 6450

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 6.6.1; 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
```

40 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 transitions 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 can 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 must be set to 255 only if this router is the actual owner of the virtual router IP address.
preempt	Specifies that a higher priority router can preempt a lower priority master router.
no preempt	Specifies that a higher priority router cannot preempt a lower priority master router.
seconds	The interval in seconds after which the master router sends VRRP advertisements. The advertising interval must be same for all VRRP routers configured with the same VRID. The valid range is 1 to 255 seconds.

Defaults

parameter	default
enable | disable | on | off	**disable** (**off**)
priority	100
preempt | no preempt	**preempt**
seconds	1

Platforms Supported

OmniSwitch 6450

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 assigned with the IP address. 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 is set to the default value of 100. The IP address owner becomes 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 must be different. The **preempt** or **no preempt** setting specifies whether or not a higher priority router can preempt a lower priority master router.

Examples

```
-> vrrp 23 1 priority 75
-> vrrp 23 1 enable
```

Release History

Release 6.6.3; command 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 6450

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 6.6.3; command introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.
show vrrp statistics	Displays statistics 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 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 tracks.
slot/port	The slot/port number that this policy tracks.
address	The remote IP or IPv6 address to be tracked by this policy.

Defaults

parameter	default
enable | disable	**enable**
value	25

Platforms Supported

OmniSwitch 6450

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 6.6.3; command introduced.

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 6450

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 6.6.3; command 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 6450

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 6.6.3; command 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 must wait before they go active; the range is 0 to 180 seconds.

Defaults

parameter	default
seconds	45 seconds

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use this command to prevent loss of workstation connectivity before a virtual router becomes master.

Examples

```
-> vrrp delay 50
```

Release History

Release 6.6.3; command 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 6450

Usage Guidelines

- Modifying the default advertising interval value affects 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 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 takes priority over the new default value. To override the configured value with the new default value, you must disable the virtual routers. Now, override the configured value using the **vrrp set** command using the **override** option. Enable the virtual routers again.

Examples

```
-> vrrp interval 50
```

Release History

Release 6.6.3; command 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 to 254.

Defaults

parameter	default
priority	100

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Modifying the default priority value affects 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 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 takes priority over the new default value. To override the configured value with the new default value, you must 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 6.6.3; command 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 can preempt a lower priority master router by default.
no preempt	Specifies that a higher priority router cannot preempt a lower priority master router by default.

Defaults

parameter	default
preempt | no preempt	**preempt**

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Modifying the default preempt mode affects 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 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 takes priority over the new default value. To override the configured value with the new default value, you must 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 6.6.3; command 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 through 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 through the **vrrp group all** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- This command changes the administrative status of all the virtual routers on the switch by executing a single command.
- This command does 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 6.6.3; command 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 6450

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 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 takes priority over the new default value. To override the configured value with the new default value, you must 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 6.6.3; command 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 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 to 255.
seconds	The default advertising interval for the virtual router group. The valid range is 1 to 255 seconds.
priority	The default priority value for the virtual router group. The valid range is 1 to 254.
preempt	Specifies that a higher priority router can preempt a lower priority master router by default.
no preempt	Specifies that a higher priority router cannot preempt a lower priority master router by default.

Defaults

parameter	default
seconds	1
priority	100
preempt | no preempt	**preempt**

Platforms Supported

OmniSwitch 6450

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 does not affect 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 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 takes priority over the new default value. To override the configured value with the new default value, you must 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 de-allocation 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 6.6.3; command 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 to 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 6450

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 does 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 6.6.3; command introduced.

Related Commands

vrrp group	Creates a 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 to 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 parameter values to the new default value.
override	Overrides the parameter configured value with the group default value.

Defaults

parameter	default
interval | priority | preempt | all	**all**

Platforms Supported

OmniSwitch 6450

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 takes priority over the group default value. To override the configured value with the group default value, you must 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 6.6.3; command introduced.

Related Commands

vrrp group	Creates a 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 to 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 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 does not adopt the group default parameter values until it is re-enabled.
- 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 6.6.3; command 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 to 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 must be set to 255 only if this router is the actual owner of the virtual router IP address.
preempt	Specifies that a higher priority router can preempt a lower priority master router.
no preempt	Specifies that a higher priority router cannot preempt a lower priority master router.
accept	Specifies that the master router, which is not the IPv6 address owner must 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 does not accept the packets addressed to the IPv6 address owner as its own.
centiseconds	The interval in centiseconds after which the master router sends VRRP3 advertisements. The advertising interval must be the same for all VRRP3 routers configured with the same VRID. The valid range is 1 to 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 6450

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 centiseconds interval. A smaller interval results 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 6.6.3; command 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 to 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 6450

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 6.6.3; command 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 6450

Usage Guidelines

SNMP traps must be enabled globally on the switch for VRRP3 traps to be sent.

Examples

```
-> vrrp3 trap
-> no vrrp3 trap
```

Release History

Release 6.6.3; command 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 to 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 6450

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 6.6.3; command 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 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the **show vrrp** command to display information about configuration parameters that can be set using 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 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 priority for the virtual router. For more information about priority, see the **vrrp** command description on page 40-3.
Preempt	Controls whether a higher priority virtual router blocks a lower priority master router: **Preempt** indicates that a higher priority virtual router blocks a lower priority master; **no preempt** indicates that the first backup router to take over for the master is not blocked by a virtual router with a higher priority. In either case, the IP address owner always takes over.
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 6.6.3; command introduced.

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 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 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 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 6.6.3; command 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 6450

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 6.6.3; command introduced.

Related Commands

vrrp track	Creates a 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 to 255.
track_id	The ID of the tracking policy for which you want to display information.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 is equal to the configured priority (Conf Pri) minus the tracking priority (Track Pri). Otherwise the current priority is considered to 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 6.6.3; command introduced.

Related Commands

vrrp track-association	Associates a VRRP tracking policy with a virtual router.
vrrp track	Creates a 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 to 255.

Defaults

By default, the default parameter values are displayed for all the virtual router groups.

Platforms Supported

OmniSwitch 6450

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 priority for the virtual router group. For more information about priority, see the **vrrp** command description on page 40-3.
Preempt Mode	Controls whether a higher priority virtual router can block a lower priority master; **preempt i**ndicates that a higher priority virtual router can block a lower priority master; **no preempt** indicates that the first backup router to take over for the master is not blocked by a virtual router with a higher priority. In either case, the IP address owner always takes over.

Release History

Release 6.6.3; command introduced.

Related Commands

vrrp group	Creates a 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 to 255.

Defaults

By default, all virtual router group associations are displayed.

Platforms Supported

OmniSwitch 6450

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 6.6.3; command 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 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the **show vrrp3** command to display information about configuration parameters, which can 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 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 priority for the virtual router. For more information about priority, see the **vrrp3** command description on page 40-29.
Preempt	Controls whether a higher priority virtual router blocks a lower priority master: **preempt** indicates that a higher priority virtual router can block a lower priority master; **no preempt** indicates that the first backup router to take over for the master is not blocked by a virtual router with a higher priority. In either case the IP address owner always takes over it if is available.
Accept	Displays whether the master router, which is not the IPv6 address owner, accepts 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 6.6.3; command 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 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 state has transitioned from backup to master.
Adv. Rcvd	The total number of VRRP3 advertisements received by this instance.

Release History

Release 6.6.3; command 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 to 255.
track_id	The ID of the tracking policy for which you want to display information.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

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 is equal to the configured priority (Conf Pri) minus the tracking priority (Track Pri). Otherwise the current priority is considered to 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 6.6.3; command 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
```

41 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 disables 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	Specifies source port, or range of ports desired to be mirrored.
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.
destination	Specifies the destination port, that receives all the mirrored packets.
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 6350, 6450

Usage Guidelines

- The maximum number of mirroring sessions is limited to two.
- 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. In other words, you can configure up to 24 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

- 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.
- 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 6.6.1; command was introduced.

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 6450, 6350

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 6.6.1; 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 (e.g., 3/1 specifies port 1 on slot 3).
file *filename*	Specifies a file name for the monitoring session (e.g., **/flash/port2**).
filesize	Specifies the size of the file in 16K (16384) byte increments. For example, a value of 3 would specify a size of 49152 bytes. The file size can be up to 160 K (163840 bytes).
no file	Specifies that no file will be created for the monitoring session.
on	Specifies that any existing port monitoring file in flash memory will be overwritten if the total data exceeds the specified file size.
off	Specifies that any existing port monitoring file in flash memory will not be overwritten if the total data exceeds the specified file size.
inport	Specifies incoming unidirectional port monitoring.
outport	Specifies outgoing unidirectional port monitoring.
seconds	Specifies the number of seconds 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 6450, 6350

Usage Guidelines

- The maximum number of monitoring sessions is limited to one per chassis and/or stack.

- 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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**.

output definitions (continued)

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.

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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
```

42 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 threshold port-trap
health interval
health statistics reset
show health threshold
show health threshold port-trap
show health interval
show health
show health all
show health slice

health threshold

Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, CPU usage, and chassis temperature.

Input traffic, output/input traffic, memory usage, 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.

Defaults

parameter	default
percentage	80
degrees	50

Platforms Supported

OmniSwitch 6450, 6350

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.

Note. Do not configure the port health threshold (Rx and TxRx) value close to the line rate (rate at which traffic is sent). For example, if the traffic is sent at 50 % line rate, then configure the health threshold value of about 80% and not about 60%.

- 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 42-8, or refer to the “Diagnosing Switch Problems” chapter in the *OmniSwitch AOS Release 6 Network Configuration Guide*.

Note. The console messages `"+++ healthMonCpuStatus Crossed Below The Threshold Limit "` can be seen on switch bootup if it is configured to receive health monitoring debug messages on console or swlog file using the **swlog appid** and **swlog output** commands.

- 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 6.6.1; command was introduced.

Related Commands

show health threshold	Displays the current health threshold settings.

MIB Objects

```
HealthThreshInfo
   healthThreshDeviceRxLimit
   healthThreshDeviceTxRxLimit
   healthThreshDeviceTempLimit
   healthThreshDeviceMemoryLimit
   healthThreshDeviceCpuLimit
```

health threshold port-trap

Enables or disables health threshold monitoring on a slot, port, or a range of ports.

health threshold port-trap {*slot* **|** *slot/port* **|** *slot/port1-port2***} {enable | disable}**

Syntax Definitions

slot/port	The slot number for the chassis and the physical port number on the slot. (for example, 2/1 specifies port 1 on slot 2).
slot/port1-port2	The slot number for the chassis, the physical start port number on that slot and end port on the slot. Here, *port1* refers of the start port and *port2* refers to the end port in the range of ports.
slot	The slot number on the chassis.
enable	Health monitoring port-trap is generated for the specified ports or slots.
disable	Health monitoring port-trap is not generated for the specified ports or slots.

Defaults

By default, the health threshold trap is **enabled** globally on the chassis ports.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Health threshold trap is enabled by default on all chassis ports.This command can be used to enable or disable health threshold traps on a slot, port, or a range of ports.
- Use valid slot and port numbers. If particular slots or ports are not available or not working, then, error messages are displayed.

Examples

```
-> health threshold port-trap 1 disable
-> health threshold port-trap 1/2 disable
-> health threshold port-trap 1/1-4 disable
```

Release History

Release 6.6.4; command introduced.

Related Commands

health threshold	Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, CPU usage, and chassis temperature.
show health threshold port-trap	Displays the current status of the health threshold monitoring settings for a slot, port, or a range of ports.

MIB Objects

```
healthPortTable
   healthPortSlot
   healthPortIF
   healthPortThresholdTrapStatus
```

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 6450, 6350

Usage Guidelines

Decreasing the polling interval may impact switch performance.

Examples

```
-> health interval 6
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 through 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 6.6.1; 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 threshold port-trap

Displays the current status of the health threshold monitoring settings for a slot, port, or a range of ports.

show health threshold port-trap {*slot* **|** *slot/port* **|** *slot/port1-port2***}**

Syntax Definitions

slot/port	The slot number for the chassis and the physical port number on the slot. (for example, 2/1 specifies port 1 on slot 2).
slot/port1-port2	The slot number for the chassis, the physical start port number on that slot and end port on the slot. Here, *port1* refers of the start port and *port2* refers to the end port in the range of ports.
slot	The slot number on the chassis.

Defaults

By default, the health threshold trap is **enabled** globally on the chassis ports.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use slot number value with this command, to view the health threshold information for all the ports on the slot.
- An error message "**No data for slot** *slotnum*" is displayed when there is no data available for a slot.

Example

```
-> show health threshold port-trap 1

Slot/Port   Status
----------+----------
    1/1    enabled
    1/2    enabled
    1/3    enabled
    1/4    enabled
    1/5    enabled
    .
    .
    .
    .
    1/26   enabled

-> show health threshold port-trap 2
ERROR: No data for slot 2
```

```
-> show health threshold port-trap 1/2

Slot/Port   Status
---------+----------
  1/2        disabled
```

output definitions

Slot/Port	Specifies the port number with the slot and port information.
Status	Specifies the current status of the health threshold settings for the port (**enabled** or **disabled**).

Release History

Release 6.6.4; command introduced.

Related Commands

health threshold port-trap	Enables or disables health threshold monitoring on a slot, port, or a range of ports.

MIB Objects

```
healthPortTable
   healthPortSlot
   healthPortIF
   healthPortThresholdTrapStatus
```

show health interval

Displays the current health sampling interval.

show health interval

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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 or temperature measured in degrees Celsius).
Curr	Current device bandwidth usage or temperature (measured in degrees Celsius).
1 Min Avg	Average device bandwidth usage or temperature (measured in degrees Celsius) over a 1-minute period.
1 Hr Avg	Average device bandwidth usage or temperature (measured in degrees Celsius) over a 1-hour period.
1 Hr Max	Maximum device bandwidth usage or temperature (measured in degrees Celsius) over a 1-hour period (i.e., the maximum of the 1 minute averages).

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

N/A

MIB Objects

```
healthSliceTable
   healthSliceSlot
   healthSliceSlice
   healthSliceMemoryLatest
   healthSliceCpuLatest
```

43 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 receiver
sflow sampler
sflow poller
show sflow agent
show sflow receiver
show sflow sampler
show sflow poller

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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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; 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 6.6.1; 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

sflow receiver	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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

sflow poller	Gets counter samples.

MIB Objects

```
sFlowCpTable
   sFlowCpInstance
```

44 QoS Commands

Alcatel QoS software provides a way to manipulate flows coming through the switch based on user-configured policies. The flow manipulation (referred to as *Quality of Service* or *QoS*) as simple as allowing or 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 45, "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

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 multicast disposition** **qos stats interval** **qos nms priority** **qos phones** **qos user-port** **qos dei** **qos force-yellow-priority** **qos force-yellow-802.1p** **qos force-yellow-dscp** **debug qos** **debug qos internal** **qos clear log** **qos apply** **qos revert** **qos flush** **qos reset** **qos stats reset** **show qos queue** **show qos queue statistics** **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 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** **show qos port**
Buffer Management commands	**qos register shared buffers** **qos port register profile** **show qos register**

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**) can 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***]**
[default bridged disposition {accept | deny | drop}]
[default multicast disposition {accept | deny | drop}]
[stats interval *seconds***]**
[user-port {filter | shutdown} {spoof | bpdu | rip}]
[dei]

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 can 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 6450, 6350

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 can 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 6.6.1; command 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
   alaQoSConfigDEIMarking
```

qos trust ports

Configures the global trust mode for QoS ports. Trusted ports accepts 802.1p and ToS/DSCP values in incoming packets; untrusted ports sets 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 is automatically added in the trust mode specified by this command. See page 44-44 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 6450, 6350

Usage Guidelines

- Use the **qos ports trusted** command to override the default for a particular port.
- The setting only applies to ports with incoming traffic.
- Any port configured for 802.1Q tagging is always trusted regardless of the global setting.
- Mobile ports can be assigned as untrusted ports.
- Use the **qos port default 802.1p** or **qos port default dscp** commands to specify that a value other than zero must be applied to the incoming packets. 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 6.6.1; command introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port trusted	Configures whether 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***] | 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.
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, priority-WRR, or DRR is the active queuing scheme. The range is 0 to 15.

Defaults

parameter	default
strict-priority | priority-wrr | wrr | drr	**strict-priority**
w0 w1 w2 w3 w4 w5 w6 w7	1 (best effort)

Platforms Supported

OmniSwitch 6450, 6350

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 as traffic shaping occurs at the destination ports. 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 6.6.1; command introduced.

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 can 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 6450, 6350

Usage Guidelines

An NMS application can 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 6.6.1; command 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 flash file system of the switch, 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 6450, 6350

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 by using the **swlog output** command.
- Use **show qos log** command to view the entire log at any time.

Examples

```
-> qos log console
-> qos no log console
```

Release History

Release 6.6.1; command introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
swlog output flash file-size	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 6450, 6350

Usage Guidelines

- To turn off logging, enter 0 for the number of log lines. (Note: Error messages are still logged.)
- If you change the number of log lines, you can 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 is changed at the next reboot.

Examples

```
-> qos log lines 5
-> qos log lines 0
```

Release History

Release 6.6.1; command 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 6450, 6350

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 information (default configuration), the **qos log level** command has no effect.
- To log fatal errors only, set the log level to 0.
- A high log level value has an impact on the performance of the switch.

Examples

```
-> qos log level 4
-> qos log level 0
```

Release History

Release 6.6.1; command introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
debug qos	Configures the type of QoS events that are 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 must accept the flow.
drop	Specifies that the switch must silently drop the flow.
deny	Specifies that the switch must drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option provides 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 6450, 6350

Usage Guidelines

- Use **policy action disposition** command to configure disposition for particular flows. The disposition for a particular flow overrides the global setting.
- Typically, when configuring IP filtering rules, the global default disposition must be set to **deny**. Filtering rules can 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 6.6.1; command introduced.

Related Commands

policy action disposition	Configures a disposition for a policy action.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDefaultBridgedDisposition
   alaQoSConfigAppliedDefaultBridgedDisposition
```

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 must accept the flow.
drop	Specifies that the switch must silently drop the flow.
deny	Specifies that the switch must drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option provides 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 6450, 6350

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 overrides the global setting.

Examples

```
-> qos default multicast disposition deny
```

Release History

Release 6.6.1; command introduced.

Related Commands

policy action disposition	Configures a disposition for a policy action.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigDefaultMulticastDisposition
   alaQoSConfigAppliedDefaultMulticastDisposition
```

qos stats interval

Configures how often the switch polls network interfaces for statistics about QoS events.

qos stats interval *seconds*

Syntax Definitions

seconds	The number of seconds before the switch polls network interfaces for statistics. The range is 10–3600.

Defaults

parameter	default
seconds	60

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command 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 6450, 6350

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. The precedence is determined only 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 6.6.1; command 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 {trusted | priority *priority_value***}**

qos no phones

Syntax Definitions

trusted	Trusts the 802.1p and DSCP prioritization on the incoming packets.
priority_value	The priority given to scheduling traffic on the output port. Value ranges from 0 (lowest) to 7 (highest).

Defaults

parameter	default
trusted	enabled
priority_value	5

Platforms Supported

OmniSwitch 6450, 6350

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. The IP phone ranges are:

MAC Address Range	Description
00:80:9F:00:00:00 to 00:80:9F:FF:FF:FF	Enterprise IP Phones Range
78:81:02:00:00:00 to 78:81:02:FF:FF:FF	Communications IP Phones Range
00:13:FA:00:00:00 to 0:13:FA:FF:FF:FF	Lifesize IP Phones Range
48-7A-55-00-00-00 to 48-7A-55-FF-FF-FF	ALE 8008 IP Phone MAC Range

- To apply the QoS IP phone priority to other, non-IP phone traffic automatically, add the source MAC addresses of such traffic to the QoS “alaPhones” 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 no phones
```

Release History

Release 6.6.1; command introduced.

Related Commands

show qos config	Displays the QoS configuration for the switch.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigAutoPhones
```

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 | bpdu | rip | 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; if these two items do not match, the packet is dropped. Also applies to ARP packets.
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.
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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to disable the filter or shutdown function. This form of the command affects 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 (for example, **spoof bpdu rip**).
- 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 bdpu rip
-> qos no user-port shutdown
```

Release History

Release 6.6.1; command introduced.

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 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 egress

qos no dei egress

Syntax Definitions

egress	Marks the DEI/CFI bit for egress packets if TCM marked the packets yellow.

Defaults

By default, no DEI/CFI bit marking is done.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to disable the global DEI bit marking (egress) configuration for the switch.
- Use the **qos port dei** command to set the DEI bit marking configuration for a specific port. 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.
- DEI mapping of ingress traffic (**qos port dei ingress**) is not supported.

Examples

```
-> qos dei egress
-> qos no dei egress
```

Release History

Release 6.6.2; command introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port dei	Configures the Drop Eligible Indicator (DEI) bit 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
   alaQoSConfigDEIMarking
```

qos force-yellow-priority

Configures equal scheduling of yellow traffic on all the egress queues.

qos force-yellow-priority *priority_value*

qos no force-yellow-priority

Syntax Definitions

priority_value	The priority value for yellow traffic. Value ranges from 0 (lowest) to 7 (highest).

Defaults

By default, the priority value is set to 0.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove the equal scheduling of yellow traffic.
- This configuration is global, and cannot be configured on per port basis.

Examples

```
-> qos force-yellow-priority 1

-> qos no force-yellow-priority
```

Release History

Release 6.6.3; command introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port dei	Configures the Drop Eligible Indicator (DEI) bit 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
   alaQoSConfigForceYellowPriority
```

qos force-yellow-802.1p

Configures equal scheduling of yellow traffic on all the egress queues. This command enables you to set 802.1p priority value for yellow traffic on OmniSwitch.

qos force-yellow-802.1p *num*

qos no force-yellow-802.1p

Syntax Definitions

num	The priority value for 802.1p priority. Value ranges from 0 (lowest) to 7 (highest).

Defaults

By default, the priority value is set to none.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove the 802.1p priority value for yellow traffic.
- This configuration is global, and cannot be configured on per port basis.

Examples

```
-> qos force-yellow-802.1p 2
-> qos no force-yellow-802.1p
```

Release History

Release 6.7.2; command introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos force-yellow-priority	Configures equal scheduling of yellow traffic on all the egress queues.
qos force-yellow-dscp	Configures equal scheduling of yellow traffic on all the egress queues. This command enables you to set DSCP priority value for yellow traffic on OmniSwitch.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigForceYellowUserPriority
```

qos force-yellow-dscp

Configures equal scheduling of yellow traffic on all the egress queues. This command enables you to set DSCP priority value for yellow traffic on OmniSwitch.

qos force-yellow-dscp *num*

qos no force-yellow-dscp

Syntax Definitions

num	The priority value for DSCP priority. Value ranges from 0 (lowest) to 63 (highest).

Defaults

By default, the priority value is set to none.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove the DSCP priority value for yellow traffic.
- This configuration is global, and cannot be configured on per port basis.

Examples

```
-> qos force-yellow-dscp 5
-> qos no force-yellow-dscp
```

Release History

Release 6.7.2; command introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos force-yellow-priority	Configures equal scheduling of yellow traffic on all the egress queues.
qos force-yellow-802.1p	Configures equal scheduling of yellow traffic on all the egress queues. This command enables you to set 802.1p priority value for yellow traffic on OmniSwitch.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSConfigTable
   alaQoSConfigForceYellowDscp
```

debug qos

Configures the type of QoS events that are 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.
port	Logs events related to QoS ports.
msg	Logs QoS messages.
classifier	Logs information whenever the switch classifies a flow; if the log level is higher, more details are provided.
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.
nimsg	Logs information about QoS interfaces.

Defaults

By default basic information messages are logged (**info**). Error messages are always logged.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to change the type of messages that are 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 6.6.1; command 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.
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 6450, 6350

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 6.6.1; command introduced.

Related Commands

debug qos	Configures the type of QoS events that are 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 6450, 6350

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 many QoS events have taken place. Clearing the log makes the file easier to manage.

Examples

```
-> qos clear log
```

Release History

Release 6.6.1; command introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
debug qos	Configures the type of QoS events that are 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 are active and stored in flash).

qos apply

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- **qos apply** command is required to activate all QoS and policy commands, and 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 6.6.1; command 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 6450, 6350

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 6.6.1; command 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 6450, 6350

Usage Guidelines

- If you enter this command, the pending policy configuration is erased. If you then enter **qos apply**, the erased configuration *overwrites the applied policies and the entire policy configuration is erased.*

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 6.6.1; command 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 are 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 6450, 6350

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 6.6.1; command 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 6450, 6350

Usage Guidelines

- Use this command to reset global QoS statistics to zero. Statistics are displayed with the **show qos statistics** command.
- Use the **egress** parameter to reset only the egress CoS queue statistics to zero. Statistics are displayed with the **show qos queue** command.

Examples

```
-> qos stats reset
-> qos stats reset egress
```

Release History

Release 6.6.1; command introduced.
Release 6.6.2; **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 6450, 6350

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 6.6.1; command 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**) can 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]
[maximum bandwidth]
[maximum egress-bandwidth]
[maximum ingress-bandwidth]
[default 802.1p *value***]**
[default dscp *value***]**
[default classification {802.1p | tos | dscp}]
[dei]

Syntax Definitions

slot/port	The physical slot and port number. For example: 4/1.

Defaults

- By default, ports are not trusted.
- By default, QoS ports do not preempt queues of lower priority.

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command introduced.
Release 6.6.2; **DEI** field added.

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
   alaQoSPortDEIMarking
```

qos port trusted

Configures whether an individual port is trusted or untrusted. Trusted ports accepts the 802.1p and ToS/DSCP values in incoming packets; untrusted ports sets 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 6450, 6350

Usage Guidelines

- Use the **qos trust ports** command to set the default trust mode for all QoS ports. Use **qos port trusted** command to override the default value for QoS ports.
- 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 must be applied to the incoming packets. This value is overridden if a policy exists that specifies a different 802.1p or ToS/DSCP value for such packets.

Examples

```
-> qos port 3/1 trusted
-> qos port 4/2 no trusted
```

Release History

Release 6.6.1; command 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***] | 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 default servicing mode. Traffic is serviced based on the weight of each queue.
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, Priority 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 | priority-wrr | wrr | drr	**strict-priority**
w0 w1 w2 w3 w4 w5 w6 w7	1 (best effort)

Platforms Supported

OmniSwitch 6450, 6350

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. Servicing mode configurations can be applied to a maximum of five ports per slot.
- The servicing mode only applies to destination (egress) ports as traffic shaping occurs at the destination ports. 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 default servicing mode priority-wrr 0 10 0 9 0 0 2 3
-> 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 6.6.1; command 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
   alaQoSPortServicingMode
   alaQosPortQ0PriorityWeight
   alaQosPortQ1PriorityWeight
   alaQosPortQ2PriorityWeight
   alaQosPortQ3PriorityWeight
   alaQosPortQ4PriorityWeight
   alaQosPortQ5PriorityWeight
   alaQosPortQ6PriorityWeight
   alaQosPortQ7PriorityWeight
```

qos port q maxbw

Configures a maximum bandwidth for each of the eight COS egress queues on the specified port.

qos port *slot/port* **q***n* **maxbw** *kbps*

qos port *slot/port* **no q***n* **maxbw** *kbps*

Syntax Definitions

slot/port	The slot/port on which the COS max bandwidth is configured.
n	The number of the queue for the specified port. Range is 1 to 8.
kbps	The maximum bandwidth value (in Kbits per second). The value can be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10 k**, **10 m**, **10 g,** or **10 t**). If the value is entered in bits per second, the switch rounds the value up to the nearest thousand.

Defaults

By default the maximum bandwidth value for each queue is set to zero (port speed).

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to return the maximum bandwidth value for the specified queue to the default value (zero).
- Configuring the 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 q1 maxbw 5g
-> qos port 1/3 q2 maxb2 4g
-> qos port 2/1 q7 maxbw 50k
-> qos port 1/3 no q1 maxbw
```

Release History

Release 6.6.1; command 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
```

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 can 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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove a configured maximum egress bandwidth value from a port.
- When configuring the maximum egress bandwidth for a combo port, specify the bandwidth value in multiples of 2 Mbps.
- 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 6.6.1; command introduced.

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 can 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 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

- By default, untrusted ports sets the 802.1p bit to zero on incoming flows. Use this command to specify that a different 802.1p value must be applied to the flow.
- If there is a matching QoS policy rule that sets the priority, the default 802.1p value is not used.
- 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 6.6.1; command 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 6450, 6350

Usage Guidelines

- The value configured by this command sets the upper byte (precedence) and therefore configures the ToS/DSCP value for the port.
- If there is a matching QoS policy rule that sets the priority, the default DSCP value is not used.
- 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 6.6.1; command 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 is used to prioritize flows coming in on the port.
dscp	Specifies that DSCP value of the flow is used to prioritize flows coming in on the port.

Defaults

parameter	default
802.1p | dscp	dscp

Platforms Supported

OmniSwitch 6450, 6350

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 using this command.
- 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 can be dropped before any QoS rules can take effect for the traffic.

Examples

```
-> qos port 8/24 default classification dscp
-> qos port 7/1 default classification 802.1p
```

Release History

Release 6.6.1; command 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 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 [egress]**

qos port *slot/port* **no dei [egress]**

Syntax Definitions

slot/port	The slot number and port number of the physical port.
egress	Sets the DEI/CFI bit for egress packets if TCM has marked the packets as yellow.

Defaults

By default, no DEI/CFI bit marking is done.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to disable the DEI bit marking (egress) configuration for the specified port
- Use the **qos dei** command to set the global DEI bit marking configuration for all QoS switch ports. 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.
- DEI mapping of ingress traffic (**qos port dei ingress**) is not supported.

Examples

```
-> qos port 1/20 dei egress
-> qos port dei egress
-> qos port 1/20 no dei egress
```

Release History

Release 6.6.2; command introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos dei	Configures the global Drop Eligible Indicator (DEI) bit 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
   alaQoSConfig
   alaQoSConfigDEIMarking
   alaQoSPortDEIMarking
```

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 6450, 6350

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 Egress  Mark  Type
-----+-----+-----+------+--------------+-----+-----+--------+-------+----+------+-
1/1   Yes     No  0/ 0        DSCP        8     0     100M     -     Yes  ethernet
1/2    No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
1/3    No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
1/4    No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
1/5    No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
1/6    No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
1/7    No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
1/8    No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
```

```
1/9    No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
1/10   No     No  0/ 0        DSCP        8     0       0K     -     Yes  ethernet
1/11   No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
1/12   No     No  0/ 0        DSCP        8     0       0K     -     No   ethernet
```

```
-> show qos port 1/1
Slot/             Default Default            Queues  Bandwidth       DEI
Port Active Trust P/DSCP  Classification Deflt Total Physical Egress Mark Type
----+-----+-----+------+---------------+------+-----+---------+-----+-----+-------+
5/1  Yes    No    0/ 0    DSCP           8      0     100M      -     Yes  ethernet
```

output definitions

Slot/Port	The slot and physical port number.
Active	Whether the port is sending or 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.
Egress	The amount of egress bandwidth for the port.
DEI Mark	Whether the port sets the DEI bit for yellow (non-conforming) egress packets.
Type	The interface type: **ethernet** or **wan**.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; **DEI Mark** field added.

Related Commands

qos port	Configures a physical port for QoS.

MIB Objects

```
alaQoSPortTable
   alaQoSPortSlot
   alaQoSPortPort
   alaQoSPortEnabled
   alaQoSPortDefault8021p
   alaQoSPortDefaultDSCP
   alaQoSPortDefaultQueues
   alaQoSPortMaximumReservedBandwidth
   alaQoSPortMaximumDefaultBandwidth
   alaQoSPortDefaultClassification
   alaQoSPortDEIMarking
```

```
alaQoSClassify
   alaQoSClassifySourceInterfaceType
```

show qos queue

Displays information 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 6450, 6350

Usage Guidelines

- Use the *slot/port* parameter to display queue statistics for a specific port.
- In OmniSwitch 6350, Xmit/Drop counters will not be updated in the command output.

Examples

```
OS6450-> show qos queue 2/10
Slot/        Q             Bandwidth    Packets
Port   VPN   No  Pri   Wt  Min   Max    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
Total Xmit Packets:    184368,
Total Drop Packets:         0,


OS6350-> show qos queue 1/1
Slot/      Q         Bandwidth        Packets
Port  VPN  No Pri Wt Min   Max        Xmit Drop      Type
-----+----+--+---+--+-----+-----+---------+---------+----
1/1     0   0   0  -     -     -          0  0          PRI
1/1     0   1   1  -     -     -          0  0          PRI
1/1     0   2   2  -     -     -          0  0          PRI
1/1     0   3   3  -     -     -          0  0          PRI
1/1     0   4   4  -     -     -          0  0          PRI
1/1     0   5   5  -     -     -          0  0          PRI
Total Xmit Packets:         0,
Total Drop Packets:         0,
```

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.
Packets Xmit	The number of packets transmitted from this queue.
Packets Drop	The number of packets dropped from this queue.
Type	The type of queuing performed on this queue (**pri**, **wrr**, **drr**).
Priority	The number of high and low priority packets per queue.
Transmit/Dropped Packet/ Bytes	The number of packets and bytes transmitted or dropped per queue.
Transmit/Dropped/Mbits	The rate of Mbits transmitted or dropped per port *per queue* displayed in seconds.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; *slot/port* and **statistics** parameters added.
Release 6.6.4; *Mbits/sec* added in the output of the command.

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).
show qos queue statistics	Displays queue details including statistics on a specific port in a system.

MIB Objects

```
alaQoSQueueTable
   alaQoSQueueId
   alaQoSQueueSlot
   alaQoSQueuePort
   alaQoSQueuePortId
   alaQoSQueueType
   alaQoSQueuePriority
   alaQoSQueueMinimumBandwidth
   alaQoSQueueMaximumBandwidth
   alaQoSQueueAverageBandwidth
   alaQoSQueueMaximumDepth
   alaQoSQueueMaximumBuffers
   alaQoSQueue8021p
   alaQoSQueuePacketsSent
   alaQoSQueuePacketsDropped
   alaQoSQueueMaxLength
   alaQoSQueueAverageLength
   alaQoSQueueCurrentLength
alaQoSQueueStatsTable
   alaQoSQueueStatsEntry
   alaQoSStatsQueueId
   alaQoSQueueStatsSlot
   alaQoSQueueStatsPort
   alaQoSQueueStatsPriority
   alaQoSQueueStatsPacketsSent
   alaQoSQueueStatsPacketsDropped
   alaQoSQueueStatsBytesSent
   alaQoSQueueStatsBytesDropped
   alaQoSQueueStatsRateSent
   alaQoSQueueStatsRateDropped
```

show qos queue statistics

Displays queue details including statistics on a specific port in a system.

show qos queue statistics [*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 6450

Usage Guidelines

- Use the *slot/port* parameter to display queue statistics for a specific port.
- Use this command to display Queue details including statistics of a specific port.
- As per the current implementation, the statistics are replayed at the end of configured QoS statistics interval. For example, if a 10 second interval is configured, at 10th second the rate counter statistics (mbps/sec) are populated. In the next 10 seconds, if no traffic is sent the rate counters display zero.
- Due to hardware limitations, the counter can hold data upto 34.3 Gig Bytes (35 Bit Counter) in an interval, after that it will wrap around. After each interval this counter is reset. So the interval has to be configured appropriately to ensure the counter does not wrap.
- For 1G traffic maximum supported time interval is around 200-230 secs with max frame size. By default the interval is 60 seconds and minimum supported interval is 10 seconds.
- QoS statistics interval of 10-20 seconds interval will be ideal for all type of port speed.

Examples

```
-> show qos queue statistics 3/1
Slot/   Q        Transmit                          Dropped
Port   No  Pri   Packets        bytes  Mbits/sec  Packets       bytes  Mbits/sec
-----+---+-----+---------+------------------+---------+---------+----------------
3/1    0   High    311989      22463208    10         0          0         0
3/1    0   Low         0          0         0         0          0         0
3/1    1   High    311408      22421376    10         0          0         0
3/1    1    Low        0          0         0         0          0         0
3/1    2   High    310827      22379544    10         0          0         0
3/1    2    Low        0          0         0         0          0         0
3/1    3   High    310240      22337280    10         0          0         0
3/1    3    Low        0          0         0         0          0         0
3/1    4   High    309660      22295520    10         0          0         0
3/1    4    Low        0          0         0         0          0         0
3/1    5   High    309082      22253904    10         0          0         0
3/1    5    Low         0         0         0         0          0         0
```

```
3/1    6   High    310435      22362210    10         0          0          0
3/1    6    Low         0             0     0         0          0          0
```

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**).
Priority	The number of high and low priority packets per queue.
Transmit/Dropped Packet/ Bytes	The number of packets and bytes transmitted or dropped per queue.
Transmit/Dropped/Mbits	The rate of Mbits transmitted or dropped per port *per queue* displayed in seconds.

Release History

Release 6.6.4; command introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).
show qos queue	Displays information for all QoS queues or only for those queues associated with a specific port.

MIB Objects

```
alaQoSQueueTable
   alaQoSQueueId
   alaQoSQueueSlot
   alaQoSQueuePort
   alaQoSQueuePortId
   alaQoSQueueType
   alaQoSQueuePriority
   alaQoSQueueMinimumBandwidth
   alaQoSQueueMaximumBandwidth
   alaQoSQueueAverageBandwidth
   alaQoSQueueMaximumDepth
   alaQoSQueueMaximumBuffers
   alaQoSQueue8021p
   alaQoSQueuePacketsSent
   alaQoSQueuePacketsDropped
   alaQoSQueueMaxLength
   alaQoSQueueAverageLength
   alaQoSQueueCurrentLength
alaQoSQueueStatsTable
   alaQoSQueueStatsEntry
   alaQoSStatsQueueId
   alaQoSQueueStatsSlot
   alaQoSQueueStatsPort
   alaQoSQueueStatsPriority
   alaQoSQueueStatsPacketsSent
   alaQoSQueueStatsPacketsDropped
   alaQoSQueueStatsBytesSent
   alaQoSQueueStatsBytesDropped
   alaQoSQueueStatsRateSent
   alaQoSQueueStatsRateDropped
```

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 [*slot/slice***]**

Syntax Definitions

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

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Information for all slots/slices is displayed unless a particular slot/slice is requested.
- 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           128/0            64/64
                            13   128/0           128/24           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.

output definitions (continued)

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 6.6.1; command introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

N/A

show qos log

Displays the log of QoS events. This command also displays the packets dropped by IP Source Filter entries.

show qos log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use this command to display the current QoS log. To clear the log, use the **qos clear log** command.

Examples

```
-> show qos log
**QOS Log**
Insert rule 0
Rule index at 0
Insert rule 1
Rule index at 1
Insert rule 2
Rule index at 2
Enable rule r1 (1) 1,1
Enable rule r2 (0) 1,1
Enable rule yuba1 (2) 1,1
Verify rule r1(1)
Enable rule r1 (1) 1,1
Really enable r1
Update condition c1 for rule 1 (1)
Verify rule r2(1)
Enable rule r2 (0) 1,1
Really enable r2
Update condition c2 for rule 0 (1)
Verify rule yuba1(1)
Enable rule yuba1 (2) 1,1
Really enable yuba1
Update condition yubamac for rule 2 (1)
QoS Manager started TUE MAR 10 13:46:50 2002

Match rule 2 to 1
Match rule 2 to 2
Match rule 2 to 3
```

```
-> show qos log
**QOS Log**
9/16/01 18:09:18 [@18:09:18] rule ISF-DROP matched
9/16/01 18:09:18 Tagged. 802.1p 0
9/16/01 18:09:18 svlan 10 VRF (null) port 1/9
9/16/01 18:09:18 MAC 00:00:1E:1D:EE:14 -> E8:E7:32:77:BB:A2
9/16/01 18:09:18 TOS 0x00 (p255) 10.10.10.10 -> 10.10.10.100
9/16/01 18:09:18 [@18:09:18] rule ISF-DROP matched
```

Release History

Release 6.6.1; command 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 6450, 6350

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:
 Marking    : Disabled
Classifier:
 Default queues          : 8
 Default queue service   : strict-priority
 Trusted ports           :  No
 NMS Priority            : Yes
 NAT flow timeout        : 300 seconds
 Phones             : trusted
 Default bridged 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
Link Shutdown: none
Debug            : info
Profile setting for yellow frame:
Force Yellow QOS:
 Priority : 4
 802.1p   : 5
 DSCP     : 3
```

output definitions

QoS Configuration	Whether QoS is enabled or disabled. Configured through the **qos** command.
Marking	Whether 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 the automatic prioritization of NMS traffic is enabled or disabled. Configured through the **qos nms priority** command.
Phones	Whether IP Phone traffic is automatically trusted or assigned a priority value. Configured through the **qos phones** command.
Default bridged disposition	Whether bridged traffic that does not match any policy is accepted or denied on the switch Configured through the **qos default bridged disposition** command.
Default IGMP/MLD disposition	Whether multicast flows that do not match any policy are 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 log messages are sent to the console. Configured through the **qos log console** command.
Forward log	Whether 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 UserPorts group. Configured through the **qos user-port** command.
Shutdown	The type of traffic that triggers an administrative shutdown of the port if the port is a member of the UserPorts group. Configured through the **qos user-port** command.
Debug	The type of information that is displayed in the QoS log. Configured through the **qos dei** command. A value of **info** indicates the default debugging type.
Priority	Displays the egress queue for forced yellow traffic. Configured through **qos force-yellow-priority** command.
801p	Displays the configured 802.1p priority value for forced yellow traffic . Configured through **qos force-yellow-802.1p** command.
DSCP	Displays the configured DSCP priority value for forced yellow traffic. Configured through **qos force-yellow-dscp** command.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; **DEI Marking** field added.
Release 6.7.2; **801p and DSCP** field added.

Related Commands

qos	Enables or disables QoS. This base command can 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
   alaQoSConfigDEIMarking
   alaQosConfigServicingMode
   alaQosConfigTrustPorts
   alaQoSConfigAutoNms
   alaQoSConfigAutoPhones
   alaQoSConfigDefaultBridgedDisposition
   alaQoSConfigDefaultMulticastDisposition
   alaQoSConfigLogLines
   alaQoSConfigLogLevel
   alaQoSConfigLogConsole
   alaQoSConfigStatsInterval
   alaQosConfigUserportFilter
   alaQosConfigUserportShutdown
   alaQoSConfigDebug
```

show qos statistics

Displays statistics about the QoS configuration.

show qos statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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
  L2TP                 : 0
  L2TP Drop            : 0
  L2TP Match           : 0
```

```
Software resources
                    Applied                      Pending
         Table  CLI LDAP ACLM  Blt Total     CLI LDAP ACLM  Blt Total     Max
         rules    0    0    0    0     0       0    0    0    0     0    2048
       actions    0    0    0    0     0       0    0    0    0     0    2048
    conditions    0    0    0    0     0       0    0    0    0     0    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    8    10       2    0    0    8    10    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  1024  1024       0     0     0
```

output definitions

Events	The number of Layer 2 or Layer 3 flows transmitted on the switch.
Matches	The number of Layer 2 or Layer 3 flows that match policies.
Drops	The number of Layer 2 or Layer 3 flows that were dropped.
L2	The number of Layer 2 events, matches, and drops.
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.

output definitions (continued)

Hardware Resources	The current usage and availability of hardware resources for the QoS configuration.
L2TP	The number of L2TP packets.
L2TP Drop	The number of L2TP packets dropped.
L2TP Match	The number L2TP packets that match policies.

Release History

Release 6.6.1; command introduced.
Release 6.6.2; L2TP parameters added.

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
   alaQoSStatsDropServicesEvents
```

qos register shared buffers

Configures the number of buffers that would be shared by all ports in the switch.

qos register shared buffers <*num*>

Syntax Definitions

num	Specifies the number of shared buffers.

Defaults

The default value of shared buffers is 1500.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The acceptable values for the shared buffers limits are: 0 – 4095.
- The CLI configured value is rounded off to the nearest multiple of 4 and this updated value is configured in the switch.
- Please contact Service & Support for information on activating the buffer management feature.

Examples

```
-> qos register shared-buffers 2000
```

Release History

Release 6.6.5; command introduced.

Related Commands

qos port register profile	Configures the profile of specific ports in the switch.
show qos register	Displays the configured number of shared buffers and the profile assignment for all the ports in the switch.

MIB Objects

N/A

qos port register profile

Configures the profile of specific ports in the switch.

qos port[*slot/port***] register profile** <*num*>

Syntax Definitions

slot/port	The physical slot and port number. For example: 3/1.
num	Specifies the profile to be applied.

Defaults

Profiles	Default
Front panel 10/100/1000 ports	0
CPU port	1
Stack / Cascading port	2
10G ports / Combo ports	3

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The acceptable values for the register profile are: 0 – 7.
- Please contact Service & Support for information on activating the buffer management feature.

Examples

```
-> qos port 3/1 register profile 2
```

Release History

Release 6.6.5; command introduced.

Related Commands

qos register shared buffers	Configures the number of buffers that would be shared by all ports in the switch.
show qos register	Displays the configured number of shared buffers and the profile assignment for all the ports in the switch.

MIB Objects

N/A

show qos register

Displays the configured number of shared buffers and the profile assignment for all the ports in the switch.

show qos register

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to display the buffer tuning.
- Please contact Service & Support for information on activating the buffer management feature.

Examples

```
-> show qos register
SHARED BUFFERS:         1500
PORT         PROFILE
-------+-----------------
1/1             0
1/2             0
1/3             0
1/4             0
1/5             0
1/6             0
1/7             0
1/8             0
1/9             0
1/10            0
1/11            0
1/12            0
1/13            0
1/14            0
1/15            0
1/16            0
1/17            0
1/18            0
1/19            0
```

```
1/20            0
1/21            0
1/22            0
1/23            0
1/24            0
1/25            3
1/26            3
```

Release History

Release 6.6.5; command introduced.

Related Commands

qos register shared buffers	Configures the number of buffers that would be shared by all ports in the switch.
qos port register profile	Configures the profile of specific ports in the switch.

MIB Objects

N/A

45 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 may be created on the switch through CLI or SNMP commands, or they may be created through the PolicyView GUI application on an attached LDAP server.

Note. Rules created through PolicyView cannot be modified through the CLI; however, you can create policies in the CLI that take precedence over policies created through PolicyView.

Refer to Chapter 44, "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 rule accounting** **policy validity period** **policy condition** **policy action** **policy list** **show policy action** **show policy list** **show active policy list** **show policy condition** **show active policy rule** **show active policy rule accounting** **show active policy list accounting details** **show active policy rule meter-statistics** **show policy rule** **show policy validity period**

Group commands	**policy network group** **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** **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** **show policy service group**
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 802.1p** **policy condition tos** **policy condition dscp** **policy condition source mac** **policy condition destination mac** **policy condition source mac group** **policy condition destination mac group** **policy condition source vlan** **policy condition source vlan group** **policy condition source port** **policy condition destination port** **policy condition source port group** **policy condition destination port group**
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** **show policy classify**
Network Address Translation (NAT) commands	**policy action rewrite** **qos nat timeout** **show qos nat flows** **show qos nat counters** **qos nat flush**

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 list** **policy rule**
Traffic prioritization/shaping	**policy action shared** **policy action priority** **policy action maximum bandwidth** **policy action maximum depth** **show policy classify** **policy rule**
802.1p/ToS/DSCP tagging or mapping	**policy condition tos** **policy condition dscp** **policy condition 802.1p** **policy action cir** **policy action 802.1p** **policy action dscp** **policy rule**
Network Address Translation (NAT)	**policy condition source ip** **policy condition source ipv6** **policy rule**
Policy based port mirroring	**policy action mirror**

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] [accounting | no accounting] [log [interval** *seconds***]] [count {packets | bytes}] [trap | no trap]**

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 may be captured as part of the switch configuration.
accounting	Enable or disable accounting mode for the rule.
no accounting	Disable accounting mode for the rule.
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.

Defaults

By default, rules are not reflexive, but they are saved to the configuration.

parameter	default
enable | disable	enable
precedence	0
accounting| no-accounting	no-accounting
log	no
log interval	30 seconds
packets | bytes	packets
trap	enable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Any rule configured through this command is not active on the switch until the **qos apply** command is issued.
- A policy rule configured through the PolicyView application may not be edited in the CLI. You may, however, create a rule using the CLI with a higher precedence that will override a rule created through PolicyView.
- Use the **no** form of the command to remove the rule from the configuration. The change will not take effect, however, until the **qos apply** command is issued.
- When a flow comes into the switch, the switch examines Layer 2 source policies first; if no match is found, it examines Layer 2 destination policies; if no match is found it then examines Layer 3 policies. The precedence value only applies within the group of the same type of rules.
- If multiple rules (of the same type; that is, Layer 2 source, Layer 2 destination, or Layer 3) are configured with the same precedence, the switch evaluates the rules in the order they were created.
- 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 **copy running-config working** command is entered, or saved after a reboot. Rules are saved by default. If **no save** is entered for the rule, the policy rule will not be written to the configuration. The **save** option should be disabled only if you want to use a policy rule temporarily.

- If the **configuration snapshot** command is entered after the **policy rule** command is configured, the resulting ASCII file will include the following additional syntax for the **policy rule** command:

  from {cli | ldap | blt}

  This syntax indicates how the rule was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in rule, this setting is not configurable.

- The **log** option is useful for determining the source of attacks on the switch firewall.
- If traps are enabled for the rule, a trap is only sent when a port disable action or UserPort shutdown operation is triggered.

Examples

```
-> policy rule rule2 precedence 65535
-> policy rule rule2 validity period vp01
-> no policy rule rule2
-> policy rule rule2 no precedence
-> policy rule no validity period
```

Release History

Release 6.6.1; 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.
policy condition	Configures condition parameters.
policy action	Configures action parameters.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy rule	Displays information for policy rules configured on the switch.
show active policy rule	Displays only those policy rules that are currently being enforced on the switch.

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleName
   alaQoSRuleEnabled
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleCondition
   alaQoSRuleAction
   alaQoSRuleReflexive
   alaQoSRuleSave
   alaQoSRuleLog
   alaQoSRuleLogInterval
   alaQoSRuleCountType
   alaQoSRulePacketCount
   alaQoSRuleByteCount
   alaQoSRuleExcessPacketCount
   alaQoSRuleExcessByteCount
   alaQoSRuleAccounting
   alaQoSRulePacketRate
   alaQoSRuleBitRate
   alaQoSRuleAccPacketCount
   alaQoSRuleAccByteCount
alaQoSAppliedRuleTable
   alaQoSAppliedRuleAccounting
   alaQoSAppliedRulePacketRate
   alaQoSAppliedRuleBitRate
   alaQoSAppliedRuleAccPacketCount
   alaQoSAppliedRuleAccByteCount
   alaQoSAppliedRuleName
   alaQoSAppliedRuleEnabled
   alaQoSAppliedRuleSource
   alaQoSAppliedRulePrecedence
   alaQoSAppliedRuleCondition
   alaQoSAppliedRuleAction
   alaQoSAppliedRuleReflexive
   alaQoSAppliedRuleSave
   alaQoSAppliedRuleLog
   alaQoSAppliedRuleLogInterval
   alaQoSAppliedCountType
   alaQoSAppliedPacketCount
   alaQoSAppliedByteCount
   alaQoSAppliedExcessPacketCount
   alaQoSAppliedExcessByteCount
```

policy rule accounting

Enables the accounting mode for a rule.

policy rule *rule_name* **accounting**

policy rule *rule_name* **no accounting**

Syntax Definitions

rule_name	Specifies the name of the rule for which the user wants to enable the accounting mode.

Defaults

By default accounting is disabled.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use the **no** form of the command to disable the accounting mode for the rule.

Examples

```
-> policy rule r1 accounting
-> policy rule r1 no accounting
```

Release History

Release 6.6.4; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show active policy rule accounting	Displays the accounting results for all the rules that have the accounting mode enabled or for the particular rule specified in the command.

MIB Objects

NA

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 (e.g., Monday, Tuesday, Wednesday, etc.).
months	The month(s) in which the validity period is active. Enter the actual month (e.g., January, February, March, etc.).
hh:mm	The time of day, specified in hours and minutes, the validity period starts and the time of day the validity period ends (e.g., 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 (e.g., 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 6450, 6350

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 may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy 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 6.6.1; 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 network group

Configures a network group name and its associated IP addresses. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the network group.

policy network group *net_group ip_address* **[mask** *net_mask***] [***ip_address2* **[mask** *net_mask2***]...]**

no policy network group *net_group*

policy network group *net_group* **no** *ip_address* **[mask** *netmask***] [***ip_address2* **[mask** *net_mask2***]...]**

Syntax Definitions

net_group	The name of the network group (up to 31 alphanumeric characters).
ip_address	An 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 may 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 6450, 6350

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 may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in network group, this setting is not configurable.

Examples

```
-> policy network group webgroup1 10.10.12.5 10.50.3.1
-> policy network group webgroup1 no 10.10.12.5
-> no policy network group webgroup1
```

Release History

Release 6.6.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A network group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy network group	Displays information for policy network groups.

MIB Objects

```
alaQoSNetworkGroupsTable
   alaQoSNetworkGroupsName
   alaQoSNetworkGroupsSource
alaQoSAppliedNetworkGroupsTable
   alaQoSAppliedNetworkGroupsName
   alaQoSAppliedNetworkGroupsSource
alaQoSNetworkGroupTable
   alaQoSNetworkGroupIpAddr
   alaQoSNetworkGroupsIpMask
alaQoSAppliedNetworkGroupTable
   alaQoSAppliedNetworkGroupIpAddr
   alaQoSAppliedNetworkGroupsIpMask
```

policy service group

Configures a service group and its associated services. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the service group.

policy service group *service_group service_name1* **[***service_name2...***]**

no policy service group *service_group*

policy service group *service_group* **no** *service_name1* **[***service_name2...***]**

Syntax Definitions

service_group	The name of the service group (up to 31 alphanumeric characters).
service_name1	The service name is configured through the **policy service** command and includes information about protocol, source port, and destination port.
service_name2...	Optional. Additional service names may be configured for a service group. Separate each service name with a space.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in service group, this setting is not configurable.

Examples

```
-> policy service group servgroup2 telnet ftp
-> policy service group servgroup2 no telnet
-> no policy service group servgroup2
```

Release History

Release 6.6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy service	Configures a service that may be used as part of a policy service group.
policy condition	Configures a policy condition. A network group may be configured as part of a policy condition.
show policy service group	Displays information for policy service groups.

MIB Objects

```
alaQoSServiceGroupsTable
   alaQoSServiceGroupsName
   alaQoSServiceGroupsSource
alaQoSAppliedServiceGroupsTable
   alaQoSAppliedServiceGroupsName
   alaQoSAppliedServiceGroupsSource
alaQoSServiceGroupTable
   alaQoSServiceGroupServiceName
alaQoSAppliedServiceGroupTable
   alaQoSAppliedServiceGroupServiceName
```

policy mac group

Configures a MAC group and its associated MAC addresses. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the MAC group.

policy mac group *mac_group mac_address* **[mask** *mac_mask***] [***mac_address2* **[mask** *mac_mask2***]...]**

no policy mac group *mac_group*

policy mac group *mac_group* **no** *mac_address* **[mask** *mac_mask***] [***mac_address2* **[mask** *mac_mask2***]...]**

Syntax Definitions

mac_group	The name of the MAC group (up to 31 alphanumeric characters).
mac_address	The MAC address associated with the group (for example, 00:20:da:05:f6:23).
mac_mask	The mask of the MAC address, used to identify which bytes in the MAC address are significant when comparing the MAC address in the received frame with the MAC address in the policy condition. If no mask is specified, the switch automatically uses ff:ff:ff:ff:ff:ff.
mac_address2	Optional. Additional MAC addresses may be configured for a MAC group. Separate each address with a space.
mac_mask2	The mask of an additional MAC address, used to identify which bytes in the MAC address are significant when comparing the MAC address in the received frame with the MAC address in the policy condition. If no mask is specified, the switch automatically uses ff:ff:ff:ff:ff:ff.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- If the **snapshot** command is entered after the **policy map group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy map group** command:

  from {cli | ldap | blt}

This syntax indicates how the map group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy mac group mac_group1 00:20:da:05:f6:23 00:20:da:05:f6:24
-> no policy mac group mac_group1
```

Release History

Release 6.6.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A MAC group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy mac group	Displays information about policy MAC groups.

MIB Objects

```
alaQoSMACGroupsTable
   alaQoSMACGroupsName
   alaQoSMACGroupsSource
alaQoSAppliedMACGroupsTable
   alaQoSAppliedMACGroupsName
   alaQoSAppliedMACGroupsSource
alaQoSMACGroupTable
   alaQoSMACGroupMacAddr
   alaQoSMACGroupMacMask
alaQoSAppliedMACGroupTable
   alaQoSAppliedMACGroupMacAddr
   alaQoSAppliedMACGroupMacMask
```

policy port group

Configures a port group and its associated slot and port numbers. A port group may be attached to a policy condition. The action associated with that policy will be applied to all members of the port group. This command can be used to specify a rate limiter for the group of ports or individual port by specifying the mode for the port group.

policy port group *group_name* **[mode {split | non-split}]** *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).
split	The policy action is applied on individual port.
non-split	The policy action is applied on the port group.
*slot/port***[-***port***]**	The slot and port (or port range) to be included in the group. At least one slot/port combination must be specified. Additional combinations may be included in the group; each combination should be separated by a space.

Defaults

By default, non-split mode is the default behavior for the source port group.

Platforms Supported

OmniSwitch 6450, 6350

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* (For example, 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 and/or, BPDU) 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 may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.
- Per port rate limiting is limited to the source port group attached to the default policy list. The configuration is not valid for any other policy list. Hence, the configuration of the policy rule for the split mode is not valid for the explicit policy lists including ingress policy list.
- Policy action ‘shared’ cannot be used with the rule where split source port group is configured.
- Rate limiting is not supported for destination port group.
- Maximum bandwidth policies are applied to source (ingress) ports or flows. This applies to flows that involve more than one port. Based on the rate limit mode set on the port group, the maximum bandwidth is applied. For more information on this, refer to ‘Port Groups and Maximum Bandwidth’ section in the “Configuring QoS” chapter of *OmniSwitch AOS Release 6 Network Configuration Guide.*

Examples

```
-> policy port group port_group4 3/1-2 4/3 5/4
-> policy port group port_group4 mode split 3/1-2
-> policy port group port_group4 mode non-split 2/1-2 5/3 5/1-6
-> policy port group port_group4 no 3/1-2
-> policy port group UserPorts 4/1-8 5/1-8
-> no policy port group pg1
```

Release History

Release 6.6.1; command was introduced.
Release 6.6.5; ‘mode’ parameter added.

Related Commands

policy condition	Configures a policy condition. A port group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
policy action maximum bandwidth	Configures a maximum bandwidth value for a policy action.
show policy port group	Displays information about policy port groups.
show active policy rule	Displays information about applied policy rules that are active (enabled) on the switch, and per port statistics.
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).

MIB Objects

```
alaQoSPortGroupsTable
   alaQoSPortGroupsName
   alaQoSPortGroupsSource
   alaQoSPortGroupsStatus
   alaQoSPortGroupsMode
alaQoSAppliedPortGroupsTable
   alaQoSAppliedPortGroupsName
   alaQoSAppliedPortGroupsSource
alaAppliedPortGroupTable
   alaQoSAppliedPortGroupSlot
   alaQoSAppliedPortGroupPort
   alaQoSAppliedPortGroupPortEnd
```

policy vlan group

Configures a VLAN group and its associated VLAN ID numbers. A VLAN group may 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 vlanstart***[-***vlanend***] [***vlanstart2***[-***vlanend2***]...]**

no policy vlan group *group_name*

policy vlan group *group_name* **no** *vlanstart***[-***vlanend***] [***vlanstart2***[-***vlanend2***]...]**

Syntax Definitions

group_name	The name of the VLAN group (up to 31 alphanumeric characters).
*vlanstart***[-***vlanend***]**	The VLAN (or VLAN range) to be included in the group. At least one VLAN 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 6450, 6350

Usage Guidelines

- Use the **no** form of the command to remove a VLAN group from the configuration, or to remove a VLAN from a VLAN group.
- Use this command to configure a group of inner and/or outer VLAN to which you want to apply QoS rules. Rather than creating a condition for each VLAN, group VLANs together. Use the **policy condition** command to associate a condition with the VLAN group.
- If a range of VLANs is specified using the syntax *vlanstart-vlanend* (For example, 100-120), 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 may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy 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 6.6.2; command was introduced.

Related Commands

policy condition source vlan	Configures a source VLAN policy condition. A VLAN group may 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 may be referenced in a policy action with the **map** keyword.

policy map group *map_group* **{***value1***:***value2***...}**

no policy map group *map_group*

policy map group no {*value1***:***value2***...}**

Syntax Definitions

map_group	The name of the map group (up to 31 alphanumeric characters).
value1	The 802.1p, ToS, or DSCP value to be mapped to another value. May be a value or a range of values (for example, **1-2**).
value2...	The 802.1p, ToS, or DSCP value to be used in place of *value1*. Additional mapping pairs may be included.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove a mapping pair or to remove the map group entirely.
- The map group may 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 may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy map group tosGroup 1-4:3 5-6:5 7:6
-> policy map group tosGroup no 7:6
-> no policy map group tosGroup
```

Release History

Release 6.6.1; 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 may be used as part of a policy service group or included as part of a policy condition. A service is a source and/or destination TCP or UDP port or port range.

This overview section describes the base command. *At least one option must be configured with the base command.* Some options may be used in combination; some options are shortcuts for keyword combinations (see the Usage Guidelines). Options are described as separate commands. See the command descriptions and usage guidelines for valid combinations.

Use the **no** form for keywords to remove a parameter from a service.

policy service *service_name*
[protocol *protocol***]**
[source ip port *port***[-***port***]]**
[destination ip port *port***[-***port***]]**
[source tcp port *port***[-***port***]]**
[destination tcp port *port***[-***port***]]**
[source udp port *port***[-***port***]]**
[destination udp port *port***[-***port***]]**

no policy service *service_name*

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
protocol	The protocol associated with the service. The range of values is 0–255. Currently a value of 6 (for TCP) or 17 (for UDP) is supported. This value must be specified for **source ip port** or **destination ip port**; it cannot be specified for **source tcp port**, **destination tcp port**, **source udp port**, or **destination udp port**.
port	The well-known port number (or port range) for the desired service. For example, the port number for Telnet is 23. Specify a range of ports using a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.

- The command options offer alternate ways of configuring TCP or UDP ports for a service. Note that port types (TCP or UDP) cannot be mixed in the same service. The following table shows how the keywords are used:

To configure:	Use keywords:	Notes
TCP or UDP ports for a service	**protocol** **source ip port** **destination ip port**	*The protocol must be specified with at least one source or destination port.*
TCP ports for a service	**source tcp port** **destination tcp port**	*Keywords may be used in combination.*
UDP ports for a service	**source udp port** **destination udp port**	*Keywords may be used in combination.*

- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

The following two commands show two different ways of configuring the same service:

```
-> policy service telnet2 protocol 6 destination ip port 23
-> policy service telnet3 destination tcp port 23
```

Release History

Release 6.6.1; 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 may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **protocol** *protocol* **{[source ip port** *port***[-***port***]] [destination ip port** *port***[-***port***]]}**

no policy service *service_name*

policy service *service_name* **[no source ip port] [no destination ip port]**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
protocol	The protocol associated with the service. The range of values is 0–255. Currently a value of 6 (for TCP) or 17 (for UDP) is supported.
port	The well-known port number (or port range) for the desired service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. (A protocol value cannot be removed from a service.)
- Shortcut commands for the **policy service protocol** command include the following: **policy service source tcp port**, **policy service destination tcp port**, **policy service source udp port**, and **policy service destination udp port**.
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service telnet2 protocol 6 destination ip port 23 source ip port 22
-> policy service telnet2 no source ip port
```

Release History

Release 6.6.1; 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 may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **source tcp port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no source tcp port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired TCP service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.
- Ports associated with a particular service must all be of the same type. (The **destination tcp port** keyword may be used with this command; other keywords for the command are not allowed.)
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service serv_5 source tcp port 21-22
```

Release History

Release 6.6.1; 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 may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **destination tcp port** *port***[**-*port***]**

no policy service *service_name*

policy service *service_name* **no destination tcp port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired TCP service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 may be grouped in a policy group using the **policy service group** command. A policy condition may 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 may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service service4 destination tcp port 23
```

Release History

Release 6.6.1; 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 may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **source udp port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no source udp port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired UDP service. A port range should be separated by a hyphen (for example, **22-23**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.
- Ports associated with a particular service must all be of the same type. (The **destination tcp port** keyword may be used with this command; other keywords for the command are not allowed.)
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service serv_a source udp port 1000
-> no policy service serv_a
```

Release History

Release 6.6.1; 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 may be used as part of a policy service group or included as part of a policy condition.

policy service *service_name* **destination udp port** *port***[-***port***]**

no policy service *service_name*

policy service *service_name* **no destination udp port**

Syntax Definitions

service_name	The name of the service (up to 31 alphanumeric characters).
port	The well-known port number (or port range) for the desired UDP service. For example, a port number for NETBIOS is 137. A port range should be separated by a hyphen (for example, **137-138**).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- A policy service may be grouped in a policy group using the **policy service group** command. A policy condition may then be associated with the service group.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service.
- If the **snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy service service4 destination udp port 137
```

Release History

Release 6.6.1; 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 may be configured when the condition is created; or parameters may be configured for an existing condition. At least one parameter must be configured for a condition.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the **no** form for keywords to remove a parameter from the condition.

Some condition parameters may not be supported depending on the platform you are using. Also some condition parameters may not be supported with some action parameters. See the condition/action tables in 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]
[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***]**
[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***]**

no policy condition *condition_name*

Syntax Definitions

condition_name	The name of the condition. Any alphanumeric string.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- A policy condition and a policy action are combined to make a policy rule. See the **policy rule** command page 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.
- Use the **no** form of the command to remove a condition from a policy rule.
- At least one parameter must be associated with a condition.
- If the **snapshot** command is entered after the **policy condition** command is configured, the resulting ASCII file will include the following additional syntax for the **policy condition** command:

  from {cli | ldap | blt}

  This syntax indicates how the condition was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in condition, this option is not configurable.

Examples

```
-> policy condition cond4 source port 3/1
```

Release History

Release 6.6.1; 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
   alaQoSConditionDestinationVlan
   alaQoSCondition8021p
   alaQoSConditionSourceIpAddr
   alaQoSConditionSourceIpMask
   alaQoSConditionSourceNetworkGroup
   alaQoSConditionDestinationIpAddr
   alaQoSConditionDestinationIpMask
   alaQoSConditionDestinationNetworkGroup
   alaQoSConditionMulticastIpAddr
   alaQoSConditionMulticastIpMask
   alaQoSConditionMulticastNetworkGroup
   alaQoSConditionTos
   alaQoSConditionDscp
   alaQoSConditionTcpFlags
   alaQoSConditionIpProtocol
   alaQoSConditionSourceIpPort
   alaQoSConditionSourceIpPortEnd
   alaQoSConditionDestinationIpPort
   alaQoSConditionDestinationIpPortEnd
   alaQoSConditionSourceTcpPort
   alaQoSConditionSourceTcpPortEnd
   alaQoSConditionDestinationTcpPort
   alaQoSConditionDestinationTcpPortEnd
   alaQoSConditionSourceUdpPort
```

```
   alaQoSConditionSourceUdpPortEnd
   alaQoSConditionDestinationUdpPort
   alaQoSConditionDestinationUdpPortEnd
   alaQoSConditionService
   alaQoSConditionServiceStatus
   alaQoSConditionServiceGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSource
   alaQoSAppliedConditionSourceSlot
   alaQoSAppliedConditionSourcePort
   alaQoSAppliedConditionSourcePortEnd
   alaQoSAppliedConditionSourcePortGroup
   alaQoSAppliedConditionDestinationSlot
   alaQoSAppliedConditionDestinationPort
   alaQoSAppliedConditionDestinationPortEnd
   alaQoSAppliedConditionDestinationPortGroup
   alaQoSAppliedConditionSourceInterfaceType
   alaQoSAppliedConditionDestinationInterfaceType
   alaQoSAppliedConditionSourceMacAddr
   alaQoSAppliedConditionSourceMacMask
   alaQoSAppliedConditionSourceMacGroup
   alaQoSAppliedConditionDestinationMacAddr
   alaQoSAppliedConditionDestinationMacMask
   alaQoSAppliedConditionDestinationMacGroup
   alaQoSAppliedConditionSourceVlan
   alaQoSAppliedConditionSourceVlanGroup
   alaQoSAppliedConditionDestinationVlan
   alaQoSAppliedCondition8021p
   alaQoSAppliedConditionSourceIpAddr
   alaQoSAppliedConditionSourceIpMask
   alaQoSAppliedConditionSourceNetworkGroup
   alaQoSAppliedConditionDestinationIpAddr
   alaQoSAppliedConditionDestinationIpMask
   alaQoSAppliedConditionDestinationNetworkGroup
   alaQoSAppliedConditionMulticastIpAddr
   alaQoSAppliedConditionMulticastIpMask
   alaQoSAppliedConditionMulticastNetworkGroup
   alaQoSAppliedConditionTos
   alaQoSAppliedConditionDscp
   alaQoSAppliedConditionTcpFlags
   alaQoSAppliedConditionIpProtocol
   alaQoSAppliedConditionSourceIpPort
   alaQoSAppliedConditionSourceIpPortEnd
   alaQoSAppliedConditionDestinationIpPort
   alaQoSAppliedConditionDestinationIpPortEnd
   alaQoSAppliedConditionSourceTcpPort
   alaQoSAppliedConditionSourceTcpPortEnd
   alaQoSAppliedConditionDestinationTcpPort
   alaQoSAppliedConditionDestinationTcpPortEnd
   alaQoSAppliedConditionSourceUdpPort
   alaQoSAppliedConditionSourceUdpPortEnd
   alaQoSAppliedConditionDestinationUdpPort
   alaQoSAppliedConditionDestinationUdpPortEnd
   alaQoSAppliedConditionService
   alaQoSAppliedConditionServiceStatus
   alaQoSAppliedConditionServiceGroup
```

policy condition source ip

Configures a source IP address for a policy condition.

policy condition *condition_name* **source ip** *ip_address* **[mask** *netmask***]**

policy condition *condition_name* **no source ip**

Syntax Definitions

condition_name	The name of the condition.
ip_address	The source IP address of the Layer 3 flow.
netmask	The mask for the source IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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.
- This policy condition is not supported when applied to an egress policy list.

Examples

```
-> policy condition cond3 source ipv6::1234:531F:BCD2:F34A
```

Release History

Release 6.6.1; 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
   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 6450, 6350

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 6.6.1; 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 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 6450, 6350

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.
- This policy condition is not supported when applied to an egress policy list.

Examples

```
-> policy condition cond3 destination ipv6 ::1234:531F:BCD2:F34A
```

Release History

Release 6.6.1; 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
   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 6450, 6350

Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A multicast IP address and a multicast network group cannot be specified in the same condition.
- Use the **no** form of the command to remove a multicast IP address from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 multicast ip 224.1.1.1
```

Release History

Release 6.6.1; 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.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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
   alaQoSConditionMulticastNetworkGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionMulticastNetworkGroup
```

policy condition source ip port

Configures a source IP port number for a policy condition.

policy condition *condition_name* **source ip port** *port***[-***port***]**

policy condition *condition_name* **no source ip port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP or UDP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to remove a source IP port from a condition; however, at least one classification parameter must be associated with a condition.
- The protocol (TCP or UDP) must be specified in the condition, either on the same command line or in a previous command. Use the **ip protocol** keywords. See the **policy condition ip protocol** command.
- 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 6.6.1; 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) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- 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 6.6.1; 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) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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
   alaQoSConditionSourceTcpPort
   alaQoSConditionSourceTcpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceTcpPort
   alaQoSAppliedConditionSourceTcpPortEnd
```

policy condition destination tcp port

Configures a destination TCP port number for a policy condition.

policy condition *condition_name* **destination tcp port** *port***[-***port***]**

policy condition *condition_name* **no destination tcp port**

Syntax Definitions

condition_name	The name of the condition.
port	The TCP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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
   alaQoSConditionDestinationTcpPort
   alaQoSConditionDestinationTcpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionDestinationTcpPort
   alaQoSAppliedConditionDestinationTcpPortEnd
```

policy condition source udp port

Configures a source UDP port number for a policy condition.

policy condition *condition_name* **source udp port** *port***[-***port***]**

policy condition *condition_name* **no source udp port**

Syntax Definitions

condition_name	The name of the condition.
port	The UDP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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
   alaQoSConditionSourceUdpPort
   alaQoSConditionSourceUdpPortEnd
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceUdpPort
   alaQoSAppliedConditionSourceUdpPortEnd
```

policy condition destination udp port

Configures a destination UDP port number for a policy condition.

policy condition *condition_name* **destination udp port** *port***[**-*port***]**

policy condition *condition_name* **no destination udp port**

Syntax Definitions

condition_name	The name of the condition.
port	The UDP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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
   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 6450, 6350

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 6.6.1; 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
   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 6450, 6350

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**, **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 6.6.1; 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 6450, 6350

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**, **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 6.6.1; 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

policy service	Configures a service that may be used as part of a policy service group.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
show policy service	Displays information about all particular policy services or a particular policy service configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionService
alaQoSAppliedConditionTable
   alaQoSAppliedConditionService
```

policy condition service group

Associates a policy service group with a policy condition.

policy condition *condition_name* **service group** *service_group*

policy condition *condition_name* **no service group**

Syntax Definitions

condition_name	The name of the condition.
service_group	The service group name. Service groups are configured through the **policy service group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

policy condition	Creates a policy condition.
policy condition icmpcode	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 6450, 6350

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 6.6.1; 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 6450, 6350

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.
- This policy condition is not supported when applied to an egress policy list.

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 6.6.1; 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
   alaQoSConditionIpv6Traffic
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIpv6Traffic
```

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. May 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 6450, 6350

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 may not be specified.

Examples

```
-> policy condition cond2 tos 7
```

Release History

Release 6.6.1; 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. May 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 DSCP bits, in the range 0–7.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 may not be specified.

Examples

```
-> policy condition cond4 dscp 10
-> policy condition cond5 dscp 20-30
```

Release History

Release 6.6.1; 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. May be an existing condition name or a new condition.
mac_address	The source MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23)
mac_mask	Optional. The mask for the source MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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. May be an existing condition name or a new condition.
mac_address	The destination MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23).
mac_mask	Optional. The mask for the destination MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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. May be an existing condition name or a new condition.
group_name	The name of the source MAC group, configured through the **policy mac group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
mac_group	The name of the destination MAC group, configured through the **policy mac group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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. May be an existing condition name or a new condition.
vlan_id	The source VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- A source VLAN ID and a source VLAN group cannot be specified in the same condition.

Examples

```
-> policy condition cond5 source vlan 3
```

Release History

Release 6.6.1; 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
   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. May 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 45-22 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- A source VLAN ID and a source VLAN group cannot be specified in the same condition.

Examples

```
-> policy condition cond1 source vlan group vlan_group1
-> policy condition cond1 no source vlan group
```

Release History

Release 6.6.2; 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.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

```
alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionSourceVlanGroup
alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionSourceVlanGroup
```

policy condition destination vlan

Configures a destination VLAN for a policy condition. Note that this condition is supported only in combination with a multicast condition (**multicast ip**, **multicast ipv6**, or **multicast network group**).

policy condition *condition_name* **destination vlan** *vlan_id*

policy condition *condition_name* **no destination vlan**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
vlan_id	The destination VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 multicast ip any
```

Release History

Release 6.6.1; 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***[**-*802.1p_end***]**

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***[**-*802.1p_end***]**	The 802.1p value, or a range of 802.1p values, to be included in the condition. Use a hyphen to specify a range of values (e.g., 2-5). Only one entry is allowed per command line (a single 802.1p value or a range of values, not both).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to specify 802.1p or range of 802.1p values within range 0-7 (for example , 2-7) to which you want to apply QoS rules, rather than creating a condition for each 802.1p , specify 802.1p range together in 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.

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 6.6.1; command was introduced.
Release 6.6.2; 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.
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 source port

Configures a source port number for a policy condition. Use the **no** form of the command to remove a source port number from a condition.

policy condition *condition_name* **source port** *slot/port***[-***port***]**

policy condition *condition_name* **no source port**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
slot/port	The slot and port number (or range of ports) on which the frame is received.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- This policy condition is not supported when applied to an egress policy list.

Examples

```
-> policy condition cond2 source port 3/1
-> policy condition cond3 source port 3/2-4
```

Release History

Release 6.6.1; 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. Note that this condition is supported only in combination with a multicast condition (**multicast ip**, **multicast ipv6**, or **multicast network group**).

policy condition *condition_name* **destination port** *slot/port***[-***port***]**

policy condition *condition_name* **no destination port**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
slot/port	The slot and port number (or range of ports) on which the frame is received.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 is only applied to bridged traffic, it is not applied to routed traffic.

Examples

```
-> policy condition cond3 destination port 4/2 multicast ip any
-> policy condition cond4 destination port 4/3-4 multicast ipv6 any
```

Release History

Release 6.6.1; 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. May be an existing condition name or a new condition.
group_name	The name of the source port group. Port groups are configured through the **policy port group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- This policy condition is not supported when applied to an egress policy list.

Examples

```
-> policy condition cond6 source port group portgr4
```

Release History

Release 6.6.1; 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. Note that this condition is supported only in combination with a multicast condition (**multicast ip**, **multicast ipv6**, or **multicast network group**).

policy condition *condition_name* **destination port group** *group_name*

policy condition *condition_name* **no destination port**

Syntax Definitions

condition_name	The name of the condition. May be an existing condition name or a new condition.
group_name	The name of the destination port group. Port groups are configured through the **policy port group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 multicast ip any
```

Release History

Release 6.6.1; 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 action

Configures or deletes a QoS action. A QoS action describes how traffic that matches a particular QoS condition should be treated. It may specify a particular set of bandwidth and queue parameters, or it may simply specify whether the flow is allowed or denied on the switch.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the **no** form for keywords to remove the parameter from the action.

Note that some action parameters may not be supported depending on the platform you are using. Also some action parameters may not be supported with some conditions. See the condition table in 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***]**
[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***]**
{source | destination} rewrite ip *ip_address* **[mask** *netmask***]**

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 6450, 6350

Usage Guidelines

- Any condition parameters that the hardware supports will be used to classify the traffic; any condition parameters that are not supported by the hardware will not be used to classify traffic, and the event will be logged in the QoS log.
- Bandwidth and queue parameters may be specified when the action is created or may be specified as separate commands.
- Use the **qos apply** command to activate configuration changes.
- Use the **no** form of the command to remove a QoS action from the configuration.

Note. Do not apply **policy action mirror** with **disposition drop** as both these actions cannot be combined.

- If the **snapshot** command is entered after the **policy action** command is configured, the resulting ASCII file will include the following additional syntax for the **policy action** command:

  from {cli | ldap | blt}

  This syntax indicates how the action was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in action, this setting is not configurable.

Note. When a port group policy condition is applied using the **policy condition port group** command, the **policy action shared** command works only for port groups created on the same slot and ASIC. Each ASIC on a slot shares 24 ports sequentially (for example, ports 1/1 to 1/24 are part of one ASIC, port 1/25 to 1/48 belong to a different ASIC on the same slot). The port groups can be created using the **policy port group** command.

Examples

```
-> policy action action1 accept
```

Release History

Release 6.6.1; command was introduced.
Release 6.7.1 R02; **rewrite ip** parameter added.

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
      alaQoSAction8021p
      alaQoSActionTos
      alaQoSActionTosRewriteMask
      alaQoSActionDscp
      alaQoSActionMapFrom
      alaQoSActionMapTo
      alaQoSActionMapGroup
      alaQoSActionSourceRewriteIpAddr
      alaQoSActionSourceRewriteIpMask
      alaQoSActionSourceRewriteIpGroup
      alaQoSActionDestinationRewriteIpAddr
      alaQoSActionDestinationRewriteIpMask
      alaQoSActionDestinationRewriteIpGroup
   alaQoSAppliedActionTable
      alaQoSAppliedActionName
      alaQoSAppliedActionSource
      alaQoSAppliedActionDisposition
      alaQoSAppliedActionMinimumBandwidth
      alaQoSAppliedActionMaximumBandwidth
      alaQoSAppliedActionPeakBandwidth
      alaQoSAppliedActionPriority
      alaQoSAppliedActionShared
      alaQoSAppliedActionMaximumDepth
      alaQoSAppliedActionMaximumBuffers
      alaQoSAppliedActionCIR
      alaQoSAppliedActionCIRStatus
      alaQoSAppliedActionCBS
      alaQoSAppliedActionCBSStatus
      alaQoSAppliedActionPIR
      alaQoSAppliedActionPIRStatus
      alaQoSAppliedActionPBS
      alaQoSAppliedActionPBSStatus
      alaQoSAppliedAction8021p
      alaQoSAppliedActionTos
      alaQoSAppliedActionTosRewriteMask
      alaQoSAppliedActionDscp
      alaQoSAppliedActionMapFrom
      alaQoSAppliedActionMapTo
      alaQoSAppliedActionMapGroup
      alaQoSAppliedActionSourceRewriteIpAddr
      alaQoSAppliedActionSourceRewriteIpMask
      alaQoSAppliedActionSourceRewriteIpGroup
```

```
alaQoSAppliedActionDestinationRewriteIpAddr
alaQoSAppliedActionDestinationRewriteIpMask
alaQoSAppliedActionDestinationRewriteIpGroup
```

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 6450, 6350

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.
- Accounting mode is not supported for egress policy list. So if accounting mode is enabled for the rule then that rule cannot be part of egress policy list. Similarly, if a rule is part of an egress policy list, then that rule cannot have accounting mode enabled.
- 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 may 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.
- An egress policy rule supports a maximum of two destination port groups.
- 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 may 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 may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy 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 6.6.2; 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 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
   alaQoSRuleGroupPacketRate
   alaQoSRuleGroupBitRate
   alaQoSRuleGroupAccPacketCount
   alaQoSRuleGroupAccByteCount
alaQosAppliedRuleGroupsTable
   alaQosAppliedRuleGroupsName
   alaQosAppliedRuleGroupsSource
   alaQosAppliedGroupsType
   alaQosAppliedGroupsEnabled
   alaQosAppliedRuleGroupsStatus
   alaQosAppliedRuleGroupPacketRate
   alaQosAppliedRuleGroupBitRate
   alaQoSAppliedRuleGroupAccPacketCount
   alaQoSAppliedRuleGroupAccByteCount
```

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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove a disposition from an action.
- The **policy action disposition drop** & **policy action mirror** actions cannot be combined in one policy condition.
- 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 6.6.1; 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 6450, 6350

Usage Guidelines

- If multiple rules have the same action, more than one flow may be scheduled on the same queue if the queue is defined as shared; otherwise, a separate queue is created for each flow.
- Note that flows must be sent over the same virtual port for the flows to share a queue. For example, flows with the same 802.1Q tag may share the same queue.
- Use the **no** form of the command to disable sharing.

Note. When a port group policy condition is applied using the **policy condition port group** command, the **policy action shared** command works only for port groups created on the same slot and ASIC. Each ASIC on a slot shares 24 ports sequentially (for example, ports 1/1 to 1/24 are part of one ASIC, port 1/25 to 1/48 belong to a different ASIC on the same slot). The port groups can be created using the **policy port group** command.

Example

```
-> policy action action5 shared
-> policy action action5 no shared
```

Release History

Release 6.6.1; command was introduced.

Related Commands

policy action	Creates a policy action.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionShared
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionShared
```

policy action priority

Configures the priority for queuing a flow to which the QoS action applies.

policy action *action_name* **priority** *priority_value*

policy action *action_name* **no priority**

Syntax Definitions

action_name	The name of the action.
priority_value	The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 may be different from the value entered here.

Examples

```
-> policy action action1 priority 1
-> policy action action1 no priority
```

Release History

Release 6.6.1; 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 actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPriority
   alaQoSActionPriorityStatus
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPriority
   alaQoSAppliedActionPriorityStatus
```

policy action maximum bandwidth

Configures a maximum bandwidth value for a policy action.

policy action *action_name* **maximum bandwidth** *bps*

policy action *action_name* **no maximum bandwidth**

Syntax Definitions

action_name	The name of the action.
bps	The desired value for maximum bandwidth, in bits per second. The value may be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10k**). If the value is entered in bits per second, the switch rounds the value up to the nearest thousand.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to remove a maximum bandwidth value from an action.
- Note that the bandwidth may be entered in bits per second. Alternatively, the bandwidth may be entered in abbreviated units (**1k**, **2k**, etc). If the bandwidth value is entered in bytes, the switch rounds the value to the nearest thousand bytes. For example, if you enter 1 to 1024, the result is 1K. If you enter 1025 to 2048, the result is 2K.

Examples

```
-> policy action action4 maximum bandwidth 10000
-> policy action action4 maximum bandwidth 10k
-> policy action action4 no maximum bandwidth
```

Release History

Release 6.6.1; 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 classify	Creates a Tri-Color Marking (TCM) policy action.
show policy action	Displays information about actions configured on the switch.

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 may be entered as an integer (for example, **10000**) or with abbreviated units (for example, **10k**). If the value is entered in bytes, the switch rounds the value up to the nearest thousand.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove a maximum depth value from a policy action.
- Note that the bandwidth may be entered in bytes. Alternatively, the bandwidth may be entered in abbreviated units (**1k**, **2k**, etc). If the bandwidth value is entered in bytes, the switch rounds the value to the nearest thousand bytes. For example, if you enter 1 to 1024, the result is 1K. If you enter 1025 to 2048, the result is 2K.

Examples

```
-> policy action action2 maximum depth 100
-> policy action action2 no maximum depth
```

Release History

Release 6.6.1; 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 actions configured on the switch.

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), and Peak Burst Size (PBS).

policy action *action_name* **cir** *bps* **[cbs** *byte***] [pir** *bps***] [pbs** *byte***]**

policy action *action_name* **no cir** *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.

Defaults

parameter	default
bps	0
byte	0

Platforms Supported

OmniSwitch 6450, 6350

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 may 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 default value used by the switch for maximum depth is used as the default **cbs** and **pbs** value.
- The optional **pir** parameter is used to invoke the Two-Rate TCM mode; otherwise, TCM operates in the Single-Rate mode by default. Note that the **pir** value must be greater than the **cir** value when using the Two-Rate TCM mode.

Examples

```
-> policy action A3 cir 10M
-> policy action A4 cir 10M cbs 4k
-> policy action A5 cir 10M cbs 4k pir 20M pbs 40M
-> policy action A3 no cir 10M
```

Release History

Release 6.6.1; 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 list	Displays information about pending and applied policy rules that are active (enabled) on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionCIR
   alaQoSActionCBS
   alaQoSActionPIR
   alaQoSActionPBS
alaQoSAppliedActionTable
   alaQoSActionCIR
   alaQoSActionCBS
   alaQoSActionPIR
   alaQoSActionPBS
```

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 6450, 6350

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.
- An 802.1p or ToS/DSCP action always sets the packet priority. For 802.1p marking, the priority is set according to the marked 802.1p. For ToS marking, the priority is set according to the marked ToS. For DSCP marking, the priority is set according to the marked DSCP.
- A ToS action alters the packet IP ToS fields. The DSCP bits 3,4,5 are reset to 0. For example, a ToS 2 action on a packet carrying DSCP 5 will set a DSCP value of 40.

Examples

```
-> policy action action3 tos 4
-> policy action action3 no tos
```

Release History

Release 6.6.1; 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 actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionTos
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionTos
```

policy action 802.1p

Configures a value to be set in the 802.1p bits of the 802.1Q byte of an outgoing frame for traffic that matches a policy with this action.

policy action *action_name* **802.1p** *802.1p_value*

policy action *action_name* **no 802.1p**

Syntax Definitions

action_name	The name of the action.
802.1p_value	The priority value to be set in 802.1Q frames. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- An 802.1p or ToS/DSCP action always sets the packet priority. For 802.1p marking, the priority is set according to the marked 802.1p. For ToS marking, the priority is set according to the marked ToS. For DSCP marking, the priority is set according to the marked DSCP.

Examples

```
-> policy action action4 802.1p 7
-> policy action action4 no 802.1p
```

Release History

Release 6.6.1; 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 actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSAction8021p
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedAction8021p
```

policy action dscp

Configures a Differentiated Services Code Point (DSCP) value to be set in an outgoing flow for traffic that matches rules with this action.

policy action *action_name* **dscp** *dscp_value*

policy action *action_name* **no dscp**

Syntax Definitions

action_name	The name of the action.
dscp_value	The DSCP value to be set, in the range 0–63.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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.
- An 802.1p or ToS/DSCP action always sets the packet priority. For 802.1p marking, the priority is set according to the marked 802.1p. For ToS marking, the priority is set according to the marked ToS. For DSCP marking, the priority is set according to the marked DSCP.

Examples

```
-> policy action action2 dscp 61
-> policy action action2 no dscp
```

Release History

Release 6.6.1; 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 actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionDscp
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionDscp
```

policy action map

Configures a mapping group for a policy action.

policy action map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group*

policy action no map

Syntax Definitions

802.1p	Indicates that an 802.1p value should be mapped.
tos	Indicates that a ToS value should be mapped.
dscp	Indicates that a DSCP value should be mapped.
map_group	The name of the map group, configured through the **policy vlan group** command.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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.
- This policy action is not supported when applied to an egress policy list.

Examples

```
-> policy action pbr2 permanent gateway ip 10.10.2.1
-> policy action pbr2 no permanent gateway ip
```

Release History

Release 6.6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPermanentGatewayIpAddr
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPermanentGatewayIpAddr
```

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 6450, 6350

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.
- This policy action is not supported when applied to an egress policy list.

Examples

```
-> policy action pd01 port-disable
-> policy action pb02 no port-disable
```

Release History

Release 6.6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionPortdisable
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionPortdisable
```

policy action redirect port

Redirects bridged traffic 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 6450, 6350

Usage Guidelines

- Use the **no** form of the command to remove **redirect port** from the policy action.
- Redirection policies apply to bridged traffic. When redirecting traffic on VLAN A, the redirect port must belong to VLAN A (tagged or default VLAN). In other words, the ingress port and redirect port must both reside in the same VLAN.
- This policy action is not supported when applied to an egress policy list.

Examples

```
-> policy action rp01 redirect port 1/12
-> policy action rp01 no redirect port
```

Release History

Release 6.6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionRedirectSlot
   alaQoSActionRedirectPort
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionRedirectSlot
   alaQoSAppliedActionRedirectPort
```

policy action redirect linkagg

Redirects bridged traffic 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 12, "Link Aggregation Commands."

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove **redirect linkagg** from the policy action.
- Redirection policies apply to bridged traffic. When redirecting traffic on VLAN A, the redirect port must belong to VLAN A (tagged or default VLAN). In other words, the ingress port and redirect port must both reside in the same VLAN.
- This policy action is not supported when applied to an egress policy list.

Examples

```
-> policy action rp01 redirect port 1/12
-> policy action rp01 no redirect port
```

Release History

Release 6.6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionRedirectAgg
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionRedirectAgg
```

policy action no-cache

Disables logging of rule entries to the hardware cache.

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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove **no cache** from the policy action.
- Recommended for use when applied to traffic going to the switch.

Examples

```
-> policy action nc01 no-cache
-> policy action nc01 no no-cache
```

Release History

Release 6.6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   alaQoSActionNocache
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionNocache
```

policy action mirror

Mirrors ingress packets that match a mirroring policy to the specified port.

policy action *action_name* **ingress mirror** *slot/port*

policy action *action_name* **no mirror** *slot/port*

Syntax Definitions

action_name	The name of the action.
ingress	Mirrors ingress packets.
slot/port	The slot and port number that will receive the mirrored traffic.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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. If a packet qualifies for both types of sessions, the packet is copied to the destination for both sessions.
- This policy action is not supported when applied to an egress policy list.

Examples

```
-> policy action a1 mirror 1/7 (default ingress)
-> policy action a1 ingress mirror 1/7
-> policy action a1 no mirror
```

Release History

Release 6.6.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about actions configured on the switch.

MIB Objects

```
alaQoSActionTable
   alaQoSActionName
   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 may be used in combination but are described separately for ease in explanation.)

show policy classify {l2 | l3 | multicast} [applied]
[source port *slot/port***]**
[destination port *slot/port***]**
[source mac *mac_address***]**
[destination mac *mac_address***]**
[source vlan *vlan_id***]**
[destination vlan *vlan_id***]**
[source interface type {ethernet | **wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}]**
[destination interface type {ethernet | **wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}]**
[802.1p *value***]**
[source ip *ip_address***]**
[destination ip *ip_address***]**
[multicast ip *ip_address***]**
[tos *tos_value***]**
[dscp *dscp_value***]**
[ip protocol *protocol***]**
[source ip port *port***]**
[destination ip port *port***]**

Syntax Definitions

l2	Uses the Layer 2 classifier for the hypothetical packet. Typically specified for port, MAC address, VLAN, interface type, or 802.1p.
l3	Uses the Layer 3 classifier for the hypothetical packet. Typically specified for interface type, IP address, ToS or DSCP, IP protocol, or TCP/UDP port.
multicast	Uses the multicast IGMP classifier for the hypothetical packet. Typically 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.
- If a ToS value is specified, a DSCP value may not be specified.

Examples

```
-> show policy classify l3 tos 7
```

See the output example given on page 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

- Use this command to determine if the switch will classify the traffic condition specified and match it to a policy. By default the classifier only tests pending policies (policies that have not yet been applied). Use the **applied** keyword to test only those policies that have been applied.
- Use the **qos apply** command to activate policies.
- If a DSCP value is specified, a ToS value may not be specified.

Examples

```
-> show policy classify l3 dscp 63
```

See the output example given on page 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

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 45-154 for more information about the potential screen display.

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

- Information for all policy network groups displays unless *network_group* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy network group.
-	Indicates the policy network group is pending deletion.
#	Indicates that the policy network group differs between the pending/applied network groups.

Examples

```
-> show policy network group
Group Name:                   From   Entries
Switch                         blt   4.0.1.166
                                     10.0.1.166
                                     143.209.92.166
                                     192.85.3.1

+netgroup1                     cli   143.209.92.0/255.255.255.0
                                     172.28.5.0/255/255/255.0
```

output definitions

Group Name	The name of the port group, configured through the **policy network group** command.
From	The way the group was configured: **blt** indicates a built-in entry; **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView
Entries	The IP addresses associated with the network group.

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

- Information about all policy services is displayed unless *service_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy service.
-	Indicates the policy service is pending deletion.
#	Indicates that the policy service differs between the pending/applied services.

Examples

```
-> show policy service
   Service Name                From          IPProto    ScrPort    DstPort
telnet_service                 cli           6 (TCP)                   23
+ftp_service                   cli           6 (TCP)                   21
test_service                   cli           6 (TCP)                   21

-> show policy service telnet_service
   Service Name                From          IPProto    ScrPort    DstPort
telnet_service                 cli           6 (TCP)                   23

-> show applied policy service
   Service Name                From          IPProto    ScrPort    DstPort
telnet_service                 cli           6 (TCP)                   23
test_service                   cli           6 (TCP)                   21
```

output definitions

Service Name	The name of the port group, configured through the **policy service** command.
From	The way the service was configured: **blt** indicates a built-in entry; **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
IPProto	The IP protocol associated with the service.
ScrPort	A source port associated with the service.
DstPort	A destination port associated with the service.

Release History

Release 6.6.1; command was introduced.

Related Commands

policy service	Configures a service that may be used as part of a policy service group.

MIB Objects

```
alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceIpProtocol
   alaQoSServiceSourceIpPort
   alaQoSServiceDestinationIpPort
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceIpProtocol
   alaQoSAppliedSourceIpPort
   alaQoSAppliedServiceDestinationIpPort
```

show policy service group

Displays information about pending and applied policy service groups.

show [applied] policy service group [*service_group***]**

Syntax Definitions

applied	Indicates that only service groups that have been applied should be displayed.
service_group	The name of the service group for which you want to display information; or a wildcard sequence of characters for displaying information about service groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Information for all policy service groups displays unless *service_group* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy service group.
-	Indicates the policy service group is pending deletion.
#	Indicates that the policy service group differs between the pending/applied service groups.

Examples

```
-> show policy service group
Group Name:                    From   Entries
serv_group1                     cli   telnet
                                      ftp

serv_group2                     cli   telnet
```

output definitions

Group Name	The name of the port group, configured through the **policy service group** command.
From	The origin of the service group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
Entries	The services associated with the group. Services are configured through the **policy service** command.

Release History

Release 6.6.1; command was introduced.

Related Commands

policy service group	Configures a service group and its associated services. A service group may be attached to a policy condition.

MIB Objects

```
alaQoSServiceGroupsTable
   alaQoSServiceGroupsName
   alaQoSServiceGroupsSource
alaQoSAppliedServiceGroupsTable
   alaQoSAppliedServiceGroupsName
   alaQoSAppliedServiceGroupsSource
alaQoSServiceGroupTable
   alaQoSServiceGroupServiceName
alaQoSAppliedServiceGroupTable
   alaQoSAppliedServiceGroupServiceName
```

show policy mac group

Displays information about pending and applied MAC groups.

show [applied] policy mac group [*mac_group***]**

Syntax Definitions

applied	Indicates that only MAC groups that have been applied should be displayed.
mac_group	The name of the MAC group for which you want to display information; or a wildcard sequence of characters for displaying information about MAC groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Information for all policy MAC groups displays unless *mac_group* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy MAC group.
-	Indicates the policy MAC group is pending deletion.
#	Indicates that the policy MAC group differs between the pending/applied MAC groups.

Examples

```
-> show policy mac group
Group Name:                    From   Entries
pubs1                           cli   0020da:05f623
                                      0020da:05f624
                                      143.209.92.166
                                      192.85.3.1

+yuba                           cli   080020:D16E51
                                      172.28.5.0/255/255/255.0
```

output definitions

Group Name	The name of the port group, configured through the **policy mac group** command.
From	The origin of the MAC group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
Entries	The MAC addresses associated with the group.

Release History

Release 6.6.1; 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, and also the mode configured for the port group.

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 6450, 6350

Usage Guidelines

- Information for all policy port groups displays unless *group_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy port group.
-	Indicates the policy port group is pending deletion.
#	Indicates that the policy port group differs between the pending/applied port groups.

Examples

```
-> show policy port group
Group Name   From           Entries    Mode
Slot01       blt            1/1-26     non-split
pg1          cli            1/1-2      split
Pg2          cli            1/3-4      non-split
Pg3          cli            1/5-6      split
```

output definitions

Group Name	The name of the port group, configured through the **policy port group** command or built-in port groups automatically set up by the switch (**Slot01**, **Slot02**, **Slot03**, etc.).
From	The origin of the port group: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView; **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.
Mode	The mode configured for the port group.

Release History

Release 6.6.1; command was introduced.
Release 6.6.5; 'Mode' field added.

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 6450, 6350

Usage Guidelines

- Use the *group_name* parameter to display information for a specific VLAN group.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy vlan group.
-	Indicates the policy vlan group is pending deletion.
#	Indicates that the policy vlan 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 6.6.2; 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 6450, 6350

Usage Guidelines

- Information for all policy map groups displays unless *group_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy port group.
-	Indicates the policy port group is pending deletion.
#	Indicates that the policy port group differs between the pending/applied port groups.

Examples

```
-> show policy map group
Group Name                    From  Entries
+tosGroup                      cli  1-2:4
                                    4:5
```

output definitions

Group Name	The name of the map group, configured through the **policy map group** command.
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 6.6.1; command was introduced.

Related Commands

policy mac 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 6450, 6350

Usage Guidelines

- Information for all policy actions displays unless *action_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy action.
-	Indicates the policy action is pending deletion.
#	Indicates that the policy action differs between the pending/applied actions.

Examples

```
-> show policy action
                                    Bandwidth                       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 6.6.1; command was introduced.

Related Commands

policy action	Creates a policy action. A QoS action is a particular set of bandwidth and queue parameters that may 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 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 6450, 6350

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 may 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 active policy rule meter-statistics** 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 6.6.2; command was introduced.

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
```

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 6450, 6350

Usage Guidelines

- Information for all policy conditions displays unless *condition_name* is specified.
- The display may include any of the following characters:

character	definition
+	Indicates a new policy condition.
-	Indicates the policy condition is pending deletion.
#	Indicates that the policy condition differs between the pending/applied conditions.

Examples

```
-> show policy condition
Condition Name:               From   Src    ->    Dest
pcond1                         cli
*IP      :                           Any    ->    198.60.82.0/255.255.255.0

+c4                            cli
*IP      : 10.11.2.0/255/255/255.0         ->    Any
*TCP     :                           Any    ->    600


-> show policy condition c*
Condition Name:               From   Src    ->    Dest
+c4                            cli
*IP      : 10.11.2.0/255/255/255.0         ->    Any
*TCP     :                           Any    ->    600
```

output definitions

Condition Name	The name of the condition, configured through the **policy condition** command.
From	The origin of the condition: **cli** indicates that the entry was configured on the switch; **ldap** indicates the entry was configured through PolicyView.
Scr	The source address associated with the condition.
Dest	The destination address associated with the condition.

Release History

Release 6.6.1; 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
   alaQoSConditionSourceVlanGroup
   alaQoSConditionDestinationVlan
   alaQoSCondition8021p
   alaQoSConditionSourceIpAddr
   alaQoSConditionSourceIpMask
   alaQoSConditionSourceNetworkGroup
   alaQoSConditionDestinationIpAddr
   alaQoSConditionDestinationIpMask
   alaQoSConditionDestinationNetworkGroup
   alaQoSConditionMulticastIpAddr
   alaQoSConditionMulticastIpMask
   alaQoSConditionMulticastNetworkGroup
   alaQoSConditionTos
   alaQoSConditionDscp
```

```
alaQoSConditionTcpFlags
alaQoSConditionIpProtocol
alaQoSConditionSourceIpPort
alaQoSConditionDestinationIpPort
alaQoSConditionService
alaQoSConditionServiceGroup
```

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 6450, 6350

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 may or may 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 may 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 6.6.2; command was introduced.

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 active policy rule

Displays information about applied policy rules that are active (enabled) on the switch, and per port statistics.

show active [bridged | routed | multicast] policy rule [*rule_name***] [extended]**

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.
extended	Displays the statistics for each individual port specified in the policy port group.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **show policy rule** command to display inactive as well as active policy rules.
- Information for all rules is displayed unless *rule_name* is specified.
- Information for all rule types is displayed unless a keyword (**bridged**, **routed**, **multicast**) is specified.
- Applied rules may or may not be active on the switch. Applied rules are inactive if they have been administratively disabled with the **disable** option in the **policy rule** command.
- The display may include any of the following characters:

character	definition
+	Indicates that the policy rule has been modified or has been created since the last **qos apply**.
-	Indicates the policy object is pending deletion.
#	Indicates that the policy object differs between the pending/applied objects.

- A match may 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.

- This command displays the counters for each individual port only when the rule specifies a split port group as condition, else only the aggregated counter statistics is displayed for a particular rule and not each of the individual ports.
- If the split mode is not used in the rule configured with the port group and **extended** keyword is used for the display, an error message is displayed.
- The command 'show active policy rule *rule name* extended' will still show the aggregated counters for each sub-rules formed corresponding to each port configured with the source port group in the rule.

Examples

```
-> show active policy rule
Policy From  Prec Enab  Act Refl Log Trap Save Def Acc   Matches
 r1 cli     0  Yes  Yes   No  No  Yes  Yes Yes Yes   1241827
(L2/3):                                c2 -> a1

-> show active policy rule extended
   Policy      Port         Matches
   r1          1/1           4000
               1/2           5000

   r2          1/3           2000
               1/4           1000

-> show active policy rule r1 extended
   Policy   Port     Matches
   r1       1/3      6008280
            2/1      6738088
```

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 (e.g., 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

output definitions (continued)

Save	Whether the rule will be captured in an ASCII text file (using the **configuration snapshot** command), saved to the working directory after the **write memory** command or **copy running-config working** command is entered, or saved after a reboot. 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.
Green, Yellow, Red	Tri-Color Marking (TCM) statistics; the number of packets/bytes that are marked Green (low drop precedence), Yellow (high drop precedence) , and Red (always drop). Configured through the **show policy classify** command.
{L2/3}	The condition and the action associated with the rule; configured through the **policy condition** and **policy action** commands respectively.
Acc	Displays whether accounting mode is enabled or not enabled (**Yes** or **No**)
Port	Port associated with the rule.

Release History

Release 6.6.1; command was introduced.
Release 6.6.4; “accounting” was added to command output.
Release 6.6.5; ‘extended’ 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).

MIB Objects

```
alaQoSAppliedRuleTable
   alaQoSAppliedRuleEnabled
   alaQoSAppliedRuleName
   alaQoSAppliedRuleSource
   alaQoSAppliedRulePrecedence
   alaQoSAppliedRuleCondition
   alaQoSAppliedRuleAction
   alaQoSAppliedRuleReflexive
   alaQoSAppliedRuleSave
   alaQoSAppliedRuleMatches
   alaQoSAppliedRuleActive
   alaQoSAppliedRuleDefaultList
   alaQoSAppliedRuleAccounting
alaQoSExtendedRuleTable
   alaQoSExtendedRulePort
   alaQoSExtendedRuleMatches
```

show active policy rule accounting

Displays the accounting results for all the rules that have the accounting mode enabled or for the particular rule specified in the command.

show active policy rule [*rule_name***] accounting**

Syntax Definitions

rule_name	The name of the rule for which you want to display information of accounting results. ; 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 6450, 6350

Usage Guidelines

- Use the **show policy rule** command to display inactive as well as active policy rules.
- Information for all rules is displayed unless *rule_name* is specified.
- Applied rules may or may not be active on the switch. Applied rules are inactive if they have been administratively disabled with the **disable** option in the **policy rule** command.

Examples

```
show active policy rule accounting
   a) Examples :
Matches                                      Rate
Rule Name            Packets     Bytes       Packets/sec  Bits/sec
--------------------+-----------+-----------+------------+-------
r1                   12345        567890        123          4567

r2                    0            0             0           0

r3                   12345         567890        123          4567
```

output definitions

Rule Name	Displays the name of the accounting rule
Packets	Counts the number of packets that match the rule.
Bytes	Counts the number of bytes that match the rule.
Packets/sec	Displays he number of packets and the number of bytes matching a particular rule.
Bits/sec	Displays the number of bits matching a particular rule

Release History

Release 6.6.4; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSAppliedRuleTable
   alaQoSAppliedRuleName
   alaQoSAppliedRulePacketRate
   alaQoSAppliedRuleBitRate
   alaQoSAppliedRuleAccPacketCount
   alaQoSAppliedRuleAccByteCount
```

show active policy list accounting details

Displays the accounting results of all the active lists or the one specified in the command. The “detail” option will give the counters of the individual rules that are part of the list.

show active policy list [*list_name***] accounting [details]**

Syntax Definitions

list_name	The name of the list for which you want to display information of accounting results; 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 6450, 6350

Usage Guidelines

- Information for all lsit is displayed unless *list_name* is specified.
- Egress policy list is not part of this CLI as Accounting is not supported on egress list.

Examples

```
-> show active policy list accounting

                        Matches               Rate
List Name     Packets       Bytes            Packet/sec   Bits/sec
-------------+-------------+----------------+------------+------------
L1            2222          222222               333          33333
L2            4444          444444               666          66666

-> show active policy list accounting detail
                                        Matches              Rate
List Name        Rule Name      Packets     Bytes   Packets/sec        Bits/sec
--------------+--------------+-------------+-------------+------------+------
L1               R1             1111        111111    166               16666
                 R2             1111        111111    166               16666
L2               R3             2222        222222    333               33333
                 R4             2222        222222    333               333333
```

output definitions

List Name	Displays the name of the active list.
Rule Name	Displays the name of the accounting rule
Packets	Counts the number of packets that match the rule.
Bytes	Counts the number of bytes that match the rule.

output definitions (continued)

Packets/sec	Displays the number of packets/sec and the number of bytes matching a particular rule.
Bits/sec	Displays the number of bits/sec matching a particular rule

Release History

Release 6.6.4; command was introduced.

Related Commands

policy rule accounting	Enables the accounting mode for a rule.

MIB Objects

```
alaQoSAppliedRuleGroupTable
   alaQoSAppliedRuleGroupRuleName
   alaQoSAppliedRuleGroupAccPacketCount
   alaQoSAppliedRuleGroupAccByteCount
   alaQosAppliedRuleGroupPacketRate
   alaQosAppliedRuleGroupBitRate
```

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**).

show active policy rule [*rule_name***] meter-statistics [extended]**

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.
extended	Displays the statistics for each individual ports specified in the policy port group in a particular rule.

Defaults

By default, statistics are displayed for all rules.

Platforms Supported

OmniSwitch 6450, 6350

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 may or may not be active on the switch. Applied rules are inactive if they have been administratively disabled with the **disable** option in the **policy rule** command.
- Statistics are displayed for all three colors: Green, Yellow, and Red.
- 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).
- The extended keyword must be used along with the rule name in the ‘show active policy rule r1 meter-statistics’ as the extended keyword is used to view the statistics for each individual ports specified in the policy port group in a specific rule.

Examples

The following command examples display statistics for the color 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  r2:
  Green            :                  0,
  Yellow           :                  0,
  Red              :                  0,
```

```
  Matches          :                  0

Policy  r1:
  Green            :                  0,
  Yellow           :                  0,
  Red              :                  0,
  Matches          :                  0


-> show active policy rule r2 meter-statistics extended
Policy:r2,  Port:1/1
Green    :                   0,
Yellow   :                   0,
Red      :                   0,
Matches  :          0

Policy:r2,  Port:1/2
Green    :                   0,
Yellow   :                   0,
Red      :                   0,
Matches  :                   0
```

output definitions

Policy	The name of the policy rule, configured through the **policy rule** 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.
Port	Port number associated with the rule.

Release History

Release 6.6.2; command was introduced.
Release 6.6.5; ‘extended’ parameter added.

Related Commands

policy action cir	Configures a TCM policy action, including the 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
alaQoSAppliedRuleTable
   alaQoSAppliedRuleName
   alaQoSAppliedRuleGreenCount
   alaQoSAppliedRuleRedCount
   alaQoSAppliedRuleYellowCount
alaQoSExtendedRuleTable
   alaQoSRuleExtendedGreenCount
   alaQoSRuleExtendedYellowCount
   alaQoSExtendedRuleRedCount
   alaQoSRuleExtendedNonGreenCount
   alaQoSRuleExtendedNonRedCount
```

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 6450, 6350

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 list** command to display only active rules that are currently being enforced on the switch.
- The display may include any of the following characters:

character	definition
+	Indicates that the policy rule has been modified or has been created since the last **qos apply**.
-	Indicates the policy object is pending deletion.
#	Indicates that the policy object differs between the pending/applied objects.

Examples

```
show policy rule
   a) Examples :
            Policy                From  Prec Enab  Act Refl Log Trap Save Def Acc
 r1                                cli     0  Yes  Yes   No  No  Yes  Yes Yes Yes
  (L2/3):                               c2 -> a1
```

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 (e.g., 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 **copy running-config working** command is entered, or saved after a reboot. 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.
Acc	Displays whether accounting mode is enabled or not enabled, (**Yes** or **No**)

Release History

Release 6.6.1; command was introduced.
Release 6.6.4: “accounting” added to command output.

Related Commands

policy rule	Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSRuleTable
   alaQoSRuleSource
   alaQoSRulePrecedence
   alaQoSRuleCondition
   alaQoSRuleAction
   alaQoSRuleReflexive
   alaQoSRuleSave
   alaQoSRuleLog
   alaQoSRuleActive
   alaQoSRuleDefaultList
   alaQoSRuleEnabled
   alaQoSRuleAccounting
```

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 6450, 6350

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 6.6.1; 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
```

policy action rewrite

Configures the source or destination IP which needs to be rewritten to global IP.

policy action *action_name* **{source | destination} rewrite ip** *ip_address* **[mask** *netmask***]**

policy action *action_name* **no {source | destination} rewrite ip** *ip_address* **[mask** *netmask***]**

Syntax Definitions

action_name	The name of the action.
ip_address	The source or destination IP address.
netmask	The mask for the source or destination IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The rewrite IP (source/destination IP/network) must be an interface IP on the device.
- If the source IP is different and it contains the same rewrite IP and source port, as a part of NATing, the source port will be incremented by one and sent out.
- Telnet, Ping, SSH, and SNMP packets are not considered for NAT packets.
- Each rule will handle reverse NAT as well. Configuring a rule for reverse NAT is not required.

Examples

```
-> policy action natexample source rewrite ip 9.9.9.2
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

qos nat timeout	Configures the timeout value for the NAT flow.
show qos nat flows	Displays the flow inbound and outbound traffic details.

MIB Objects

```
alaQoSActionSourceRewriteIpAddr
alaQoSActionDestinationRewriteIpAddr
```

qos nat timeout

Configures the timeout value for the NAT flow. The timer controls the flow stored in the dynamic table.

qos nat timeout *timeout_value*

Syntax Definitions

timeout_value	The timeout value for the NAT flow. Timeout value can be in the range 10 and 200000 seconds.

Defaults

By default, timeout value is 300 seconds.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> qos nat timeout 100
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

policy action rewrite	Configures the source or destination IP which needs to be rewritten to global IP.

MIB Objects

```
alaQoSConfigNatTimeout
```

show qos nat flows

Displays the flow inbound and outbound traffic details.

show qos nat flows [protocol {UDP | TCP | ICMP} | outbound-ip *ip_address* **| inbound {public-ip** *ip_address* **| private-ip** *ip_address***]**

Syntax Definitions

protocol	Specify the protocol.
outbound-ip	Specify the outbound IP address.
inbound	Specify the inbound IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
    -> show qos nat flows
Max Limit Size:1024
Current Size:1           Peek Size:1

Proto  Inbound Private Inbound Public  Outbound     Inbound   Outbound FlowstartTime FlowlastTime
                                        Rx/Tx        Rx/Tx
-----+--------------+--------------+-------------+---------+--------+------------+-----------
UDP     5.5.5.5:63    20.20.20.1:1500 20.20.20.10:63 2199/2199   0/0         55s          33s


    -> show qos nat flows icmp
Max Limit Size:1024
Current Size:1           Peek Size:262

Proto  Inbound Private Inbound Public  Outbound     Inbound   Outbound FlowstartTime FlowlastTime
                                        Rx/Tx        Rx/Tx
-----+--------------+--------------+-------------+---------+--------+------------+-----------
ICMP    174.55.21.3    172.0.59.55     174.58.1.253  341/341   340/340    29s           15s

    -> show qos nat flows outbound-ip 174.58.1.253
Max Limit Size:1024
Current Size:262       Peek Size:262

Proto  Inbound Private Inbound Public  Outbound     Inbound   Outbound FlowstartTime FlowlastTime
                                        Rx/Tx        Rx/Tx
-----+--------------+--------------+-------------+---------+--------+------------+-----------
TCP  174.55.21.2:60  172.0.59.55:1500 174.58.1.253:60 127/127  0/0 2m    42s            3s
TCP  174.55.21.22:60 172.0.59.55:1520 174.58.1.253:60 127/127  0/0 2m    42s            3s
TCP  174.55.21.42:60 172.0.59.55:1540 174.58.1.253:60 127/127  0/0 2m    42s            3s
```

```
    -> show qos nat flows inbound public-ip 172.0.59.55
Max Limit Size:1024
Current Size:262       Peek Size:262

Proto Inbound Private Inbound Public  Outbound      Inbound   Outbound FlowstartTime FlowlastTime
                                        Rx/Tx        Rx/Tx
----+--------------+--------------+-------------+---------+--------+------------+-----------
TCP  174.55.21.2:60 172.0.59.55:1500 174.58.1.253:60 96/96      0/0     2m 6s             6
TCP  174.55.21.3:60 172.0.59.55:1501 174.58.2.253:60 96/96      0/0     2m 6s             6s
TCP  174.55.21.4:60 172.0.59.55:1502 174.58.3.253:60 96/96      0/0     2m 6s             6s

    -> show qos nat flows inbound private-ip 174.55.21.90
Max Limit Size:1024
Current Size:262       Peek Size:262

Proto Inbound Private Inbound Public  Outbound      Inbound   Outbound FlowstartTime FlowlastTime
                                        Rx/Tx        Rx/Tx
----+--------------+--------------+-------------+---------+--------+------------+-----------
TCP  174.55.21.90:60 172.0.59.55:1588 174.58.9.253:60 79/79     0/0      1m 53s        14s
```

output definitions

Max Limit Size	Maximum number flows that can be processed.
Current Size	The current statistics of the flows processed.
Peek Size	The history of the maximum flows processed.
Proto	The protocol of the flow processed.
Inbound Private	The inbound IP of the processed flow.
Inbound Public	The rewritten inbound IP and its corresponding layer 4 port number of the processed flow.
outbound	The outbound IP and layer 4 port number of the processed flow.
Inbound Rx/Tx	The number of packet forward NAT received and sent out.
outbound Rx/Tx	The number of packet reverse NAT received and sent out.
Flow start time	The time the flow processed and added to binding table.
Flow last time	The last time the flow received a packet and processed.

Release History

Release 6.7.1 R02; command introduced.

Related Commands

policy action rewrite	Configures the source or destination IP which needs to be rewritten to global IP.

MIB Objects

```
alaQosActionTable
   alaQosActionEntry
   alaQoSActionSourceRewriteIpAddr
   alaQosActionSourceRewriteNetworkGroup
```

show qos nat counters

Displays the match counters for the NAT flows.

show qos nat counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show qos nat counters
********** QOS COUNTERS **********
Entry Id        Dev     Match Count
1178            0               0
1180            0               0
1182            0               0
1184            0               0
1178            1               0
1180            1               0
1182            1               0
1184            1               0
********** QDS COUNTERS **********
qdsNatTxCount     : 0
qdsNatTxFailCount : 0
qdsRNatTxCount    : 0
qdsRNatTxFailCount: 0
********** IPNI COUNTERS *********
ipnatTxCount      :0
ipnatTxfail       :0
ipRnatTxCount     :0
ipRnatTxfailCount :0
```

output definitions

QOS COUNTERS	
Entry Id	The rule number.
Dev	The device number.
Match Count	The match count.
QDS COUNTERS	

output definitions (continued)

qdsNatTxCount	Packets processed under forward NAT in queue dispatcher.
qdsNatTxFailCount	Packets processed under forward NAT that failed in queue dispatcher.
qdsRNatTxCount	Packets processed under reverse NAT in queue dispatcher.
qdsRNatTxFailCount	Packets processed under reverse NAT that failed in queue dispatcher.
IPNI COUNTERS	
ipnatTxCount	Packets processed under forward NAT in IPNI module.
ipnatTxfail	Packets processed under forward NAT that failed in IPNI module.
ipRnatTxCount	Packets processed under reverse NAT in IPNI module.
ipRnatTxfailCount	Packets processed under reverse NAT that failed in IPNI module.

Release History

Release 6.7.1 R02; command introduced.

Related Commands

policy action rewrite	Configures the source or destination IP which needs to be rewritten to global IP.

MIB Objects

```
alaQoSAppliedRuleTable
   alaQoSAppliedRuleName
   alaQoSAppliedRulePacketRate
   alaQoSAppliedRuleBitRate
   alaQoSAppliedRuleAccPacketCount
   alaQoSAppliedRuleAccByteCount
```

qos nat flush

Clears the NAT flow entries.

qos nat flush

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> qos nat flush
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

show qos nat flows	Displays the flow inbound and outbound traffic details.

MIB Objects

```
alaQosConfigNATFlush
```

46 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 44, "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 6450, 6350

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).
- When an OmniSwitch is having more than two policy servers configured, the highest precedence server will be identified and the configuration of the highest precedence server will be loaded to avoid the policy recache.

Examples

```
-> policy server load
```

Release History

Release 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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

Pref Server IP addr  port enabled status primary

----+---------------+-----+-------+------+-------

255  135.254.163.31  5389    Up     Down
254  135.254.163.81  5389    Up     Up       X
254  135.254.163.110 5389    Up     Up
254  135.254.163.247 5389    Up     Up
255     143.209.0.2  5389    Up     Down
```

output definitions

Pref	The preference of the LDAP server.
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 6.6.1; 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 6450, 6350

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,
  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,
  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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

Usage Guidelines

This command displays information about policies created on directory servers only. Chapter 44, "QoS Commands," for information about configuring and displaying policies directly on the switch.

Examples

```
-> show policy server rules
Rules received via LDAP
opstate  rule name
--------+----------------------
up       OV-L3-AcceptAllPolicy
```

Fields are defined here:

output definitions

opstate	The operational status of the rule.
rule name	The name of the policy rule; only rules configured through PolicyView are displayed in this table.

Release History

Release 6.6.1; command was introduced.
Release 6.7.2.R05; command modified.

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 6450, 6350

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 destination 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 6.6.1; 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
```

47 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). Unlike unicast, which sends one packet per destination, multicast sends one packet to all devices in any subnetwork that has at least one device requesting the multicast traffic.

Alcatel's IPMS software is compatible with the following RFCs:

RFC 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'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 flood-unknown
ip multicast dynamic-control drop-all status
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-neighbor fast-convergence
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 star-g-mode status
ip multicast vlan star-g-mode status
ipv6 multicast status
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
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 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

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 6450, 6350

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 the 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 (i.e., disabled) status on the system if no VLAN is specified, by using only **ip multicast status** (e.g., ip multicast status).
- You can also restore the IP Multicast Switching and Routing to its default (i.e., disabled) status on the specified VLAN, by using only **ip multicast vlan** *vid* **status** (e.g., 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 6.6.1; 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
   alaIgmpStatus
alaIgmpVlan
   alaIgmpVlanStatus
```

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 6450, 6350

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 dynamic-control drop-all status

Enables or disables the processing of IPV4 protocol packets through the CPU.

ip multicast dynamic-control drop-all status [{enable | disable}]

Syntax Definitions

enable	The IPV4 protocol packets entering the switch is transparently forwarded without any CPU processing. This reduces the CPU load.
disable	The IPV4 protocol packets entering the switch is captured to the CPU before processing.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- On enabling this feature the IPV4 protocol packets are not trapped to the CPU. The packets are transparently forwarded.
- This feature should not be enabled if routing protocol or VRRP is configured on the switch.
- This feature has no influence on MDNS traffic since the MDNS Relay rule has higher precedence over IPV4 specific protocols.

Examples

```
-> ip multicast dynamic-control drop-all status enable
-> ip multicast dynamic-control drop-all status disable
```

Release History

Release 6.6.5; 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
   alaDynamicControlIpv4Status
```

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 6450, 6350

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 6.6.1; 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 6450, 6350

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 (i.e., 2) version on the system if no VLAN is specified, use **ip multicast version** followed by the value 0 (e.g., ip multicast version 0) or use only **ip multicast version** (e.g., ip multicast version).
- To restore the IGMP multicast version to the default (i.e., 2) version on the specified VLAN, use **ip multicast vlan** *vid* **version**, followed by the value 0 (e.g., ip multicast vlan 2 version 0) or use only **ip multicast vlan** *vid* **version** (e.g., 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 6.6.1; 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 6450, 6350

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 6450, 6350

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 (e.g. 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 6450, 6350

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 6450, 6350

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 (e.g., 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 6.6.1; 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-neighbor fast-convergence

Enable or disable IP multicast static neighbor fast convergence.

ip multicast static-neighbor fast-convergence {enable | disable}

Syntax Definitions

enable	Enable IP multicast static neighbor fast convergence.
disable	Disable IP multicast static neighbor fast convergence.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command enables fast convergence for multicast switching traffic over DHL and ERPv2.
- IP multicast fast convergence works only in standalone mode.
- Fast convergence is applicable only for IPMS static neighbors, and not applicable to forward entries created by IGMP group packets.

Examples

```
-> ip multicast static-neighbor fast-convergence enable
-> ip multicast static-neighbor fast-convergence disable
```

Release History

Release 6.7.2.R03; command introduced.

Related Commands

show ip multicast	Displays the IP Multicast Switching and Routing status.

MIB Objects

```
alaIgmpStaticNeighborTable
   alaIgmpStaticNeighborFastLearning
```

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 6450, 6350

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 (e.g., 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 6.6.1; 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 on a specified 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 (optional)	VLAN ID number (2–4094). Provide the Receiver VLAN associated using command **vlan ipmvlan.**

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 (e.g., ip multicast static-group 11.0.0.1 vlan 2 port 7).

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 receiver-vlan 20
-> no ip multicast static-group 225.11.11.11 vlan 4 port 7 receiver-vlan 30
```

Release History

Release 6.6.1; command was introduced.

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

```
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 6450, 6350

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 (125 seconds) value on the system if no VLAN is specified, use **ip multicast query-interval** followed by the value 0 (e.g., ip multicast query-interval 0) or use only **ip multicast query-interval** (e.g., ip multicast query-interval).
- To restore the IGMP query interval to its default (125 seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **query-interval**, followed by the value 0 (e.g., ip multicast vlan 2 query-interval 0) or use only **ip multicast vlan** *vid* **query-interval** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 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 (e.g., ip multicast last-member-query-interval 0) or use only **ip multicast last-member-query-interval** (e.g., ip multicast last-member-query-interval).
- To restore the IGMP last member query interval to its default (i.e., 10 tenths-of-seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **last-member-query interval** followed by the value 0 (e.g., ip multicast vlan 2 last-member-query-interval 0) or use only **ip multicast vlan** *vid* **last-member-query-interval** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 100 tenths-of-seconds) value on the system if no VLAN is specified, use **ip multicast query-response-interval** followed by the value 0 (e.g., ip multicast query-response-interval 0) or use only **ip multicast query-response-interval** (e.g., ip multicast query-response-interval).
- To restore the IGMP last member query interval to its default (i.e., 100 tenths-of-seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **query-response-interval** followed by the value 0 (e.g., ip multicast vlan 2 query-response-interval 0) or use only **ip multicast vlan** *vid* **query-response-interval** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 1 second) value on the system if no VLAN is specified, use **ip multicast unsolicited-report-interval** followed by the value 0 (e.g., ip multicast unsolicited-report-interval 0) or use only **ip multicast unsolicited-report-interval** (e.g., ip multicast unsolicited-report-interval).
- To restore the IGMP unsolicited report interval to its default (i.e., 1 second) value on the specified VLAN, use **ip multicast vlan** *vid* **unsolicited-report-interval** followed by the value 0 (e.g., ip multicast vlan 2 unsolicited-report-interval 0) or use only **ip multicast vlan** *vid* **unsolicited-report-interval** (e.g., 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 6.6.1; 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
   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 6450, 6350

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 (i.e., 90 seconds) value on the system if no VLAN is specified, use **ip multicast router-timeout** followed by the value 0 (e.g., ip multicast router-timeout 0) or use only **ip multicast router-timeout** (e.g., ip multicast router-timeout).
- To restore the IGMP router timeout to its default (i.e., 90 seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **router-timeout** followed by the value 0 (e.g., ip multicast vlan 2 router-timeout 0) or use only **ip multicast vlan** *vid* **router-timeout** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 30 seconds) value on the system if no VLAN is specified, use **ip multicast source-timeout** followed by the value 0 (e.g., ip multicast source-timeout 0) or use only **ip multicast source-timeout** (e.g., ip multicast source-timeout).
- To restore the IGMP source timeout to its default (i.e., 30 seconds) value on the specified VLAN, use **ip multicast vlan** *vid* **source-timeout** followed by the value 0 (e.g., ip multicast vlan 2 source-timeout 0) or use only **ip multicast vlan** *vid* **source-timeout** (e.g., 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 6.6.1; 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}]**

no ip multicast [vlan *vid***] querying**

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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove an IGMP querying entry on the specified VLAN or on the system and return to its default behavior.
- 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 (i.e., disabled) setting on the system if no VLAN is specified, by using only **ip multicast querying** (e.g., ip multicast querying).
- You can also restore the IGMP querying to its default (i.e., disabled) setting on the specified VLAN, by using only **ip multicast vlan** *vid* **querying** (e.g., 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
-> no ip multicast vlan 2 querying
```

Release History

Release 6.6.1; 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
   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 6450, 6350

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 (i.e., 2) value on the system if no VLAN is specified, use **ip multicast robustness** followed by the value 0 (e.g., ip multicast robustness 0) or use only **ip multicast robustness** (e.g., ip multicast robustness).
- To restore the IGMP robustness variable to its default (i.e., 2) value on the specified VLAN, use **ip multicast vlan** *vid* **robustness** followed by the value 0 (e.g., ip multicast vlan 2 robustness 0) or use only **ip multicast vlan** *vid* **robustness** (e.g., 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 6.6.1; 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}]**

no ip multicast [vlan *vid***] spoofing**

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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove an IGMP spoofing entry on the specified VLAN or on the system and return to its default behavior.
- 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 (i.e., disabled) setting on the system if no VLAN is specified, by using only **ip multicast spoofing** (e.g., ip multicast spoofing).
- You can also restore the IGMP spoofing to its default (i.e., disabled) setting on the specified VLAN, by using only **ip multicast vlan** *vid* **spoofing** (e.g., 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
-> no ip multicast vlan 2 spoofing
```

Release History

Release 6.6.1; 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
   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 6450, 6350

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.
- You can also restore the IGMP querying to its default (i.e., disabled) setting on the system if no VLAN is specified, by using only **ip multicast zapping** (e.g., ip multicast zapping).
- You can also restore the IGMP querying to its default (i.e., disabled) setting on the specified VLAN, by using only **ip multicast vlan** *vid* **zapping** (e.g., 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 6.6.1; 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 6450, 6350

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.
- You can also restore the IGMP querying to its default (i.e., disabled) setting on the system if no VLAN is specified, by using only **ip multicast proxying** (e.g., ip multicast proxying).
- You can also restore the IGMP querying to its default (i.e., disabled) setting on the specified VLAN, by using only **ip multicast vlan** *vid* **proxying** (e.g., ip multicast vlan 2 proxying).

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 6.6.1; 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
   alaIgmpProxying
alaIgmpVlan
   alaIgmpVlanProxying
```

ip multicast star-g-mode status

Enable or disable star-G mode (*, G) for IPv4 multicast switching.

ip multicast star-g-mode status {enable | disable}

Syntax Definitions

enable	Enable star-G mode on the switch.
disable	Disable star-G mode on the switch.

Defaults

By default, star-G mode is disabled on the switch.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When star-G is globally enabled, then all the flows that are learned are flushed and relearned as star-G entries.
- Disabling star-G globally will flush and relearn all the flows.
- Star-G mode must be enabled globally for enabling star-G mode per VLAN level.
- IGMPv3 must not be enabled on the switch when star-G mode is in operation at the global and per VLAN level.
- “show configuration snapshot ipms” command displays the star-G mode configuration details.

Examples

```
-> ip multicast star-g-mode status enable
-> ip multicast star-g-mode status disable
```

Release History

Release 6.7.2.R04; command introduced

Related Commands

ip multicast vlan star-g-mode status	Enable or disable star-G mode (*, G) for IPv4 multicast switching on a specific VLAN.
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 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 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.

MIB Objects

```
alaIgmpStarg
```

ip multicast vlan star-g-mode status

Enable or disable star-G mode (*, G) for IPv4 multicast switching on a specific VLAN.

ip multicast vlan *vlan-id* **star-g-mode status {enable | disable}**

Syntax Definitions

enable	Enable star-G mode on a specific VLAN.
disable	Disable star-G mode on a specific VLAN.
vlan_id	The VLAN ID in the range is 1- 4094.

Defaults

By default, star-G mode on a specific VLAN is disabled.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- IP multicast and star-G must be enabled globally for star-G mode to be enabled for a specific VLAN.
- IGMPv3 must not be enabled on the VLAN when star-G mode is in operation.
- Disabling star-G per VLAN will flush and relearn all the flows in that VLAN.
- “show configuration snapshot ipms” command displays the star-G mode configuration details.

Examples

```
-> ip multicast vlan 10 star-g-mode status enable
-> ip multicast vlan 10 star-g-mode status disable
```

Release History

Release 6.7.2.R04; command introduced

Related Commands

ip multicast star-g-mode status	Enable or disable star-G mode (*, G) for IPv4 multicast switching.
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 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 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.

MIB Objects

```
alaIgmpVlanStarg
```

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 6450, 6350

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 will override the system's configuration.
- You can also restore the MLD querying to its default (i.e., disabled) status on the system if no VLAN is specified, by using only **ipv6 multicast status** (e.g., ipv6 multicast status).
- You can also restore the MLD querying to its default (i.e., disabled) status on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **status** (e.g., 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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 will override 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 (i.e., 1) version on the system if no VLAN is specified, use **ipv6 multicast version** followed by the value 0 (e.g., ipv6 multicast version 0) or use only **ipv6 multicast version** (e.g., ipv6 multicast version).
- To restore the MLD multicast version to the default (i.e., 1) version on the specified VLAN, use **ipv6 multicast vlan** *vid* **version** followed by the value 0 (e.g., ipv6 multicast vlan 2 version 0) or use only **ipv6 multicast vlan** *vid* **version** (e.g., 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 6.6.1; 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 6450, 6350

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 6450, 6350

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 (e.g. 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 6450, 6350

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 6450, 6350

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 (e.g., 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 6.6.1; 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 6450, 6350

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 (e.g., 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 6.6.1; 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 6450, 6350

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 (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 125 seconds) value on the system if no VLAN is specified, use **ipv6 multicast query-interval** followed by the value 0 (e.g., ipv6 multicast query-interval 0) or use only **ipv6 multicast query-interval (**e.g., ipv6 multicast query-interval).
- To restore the MLD query interval to its default (i.e., 125 seconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **query-interval** followed by the value 0 (e.g., ipv6 multicast vlan 2 query-interval 0) or use only **ipv6 multicast vlan** *vid* **query-interval** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 1000 milliseconds) value on the system if no VLAN is specified, use **ipv6 multicast last-member-query-interval** followed by the value 0 (e.g., ipv6 multicast last-member-query-interval 0) or use only **ipv6 multicast last-member-query-interval** (e.g., ipv6 multicast last-member-query-interval).
- To restore the MLD last member query interval to its default (i.e., 1000 milliseconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **last-member-query interval** followed by the value 0 (e.g., ipv6 multicast vlan 2 last-member-query-interval 0) or use only **ipv6 multicast vlan** *vid* **last-member-query-interval** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 10000 milliseconds) value on the system if no VLAN is specified, use **ipv6 multicast query-response-interval** followed by the value 0 (e.g., ipv6 multicast query-response-interval 0) or use only **ipv6 multicast query-response-interval** (e.g., ipv6 multicast query-response-interval).
- To restore the MLD last member query interval to its default (i.e., 10000 milliseconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **query-response-interval** followed by the value 0 (e.g., ipv6 multicast vlan 2 query-response-interval 0) or use only **ipv6 multicast vlan** *vid* **query-response-interval** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 1 second) value on the system if no VLAN is specified, use **ipv6 multicast unsolicited-report-interval** followed by the value 0 (e.g., ipv6 multicast unsolicited-report-interval 0) or use only **ipv6 multicast unsolicited-report-interval** (e.g., ipv6 multicast unsolicited-report-interval).
- To restore the MLD unsolicited report interval to its default (i.e., 1 second) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **unsolicited-report-interval** followed by the value 0 (e.g., ipv6 multicast vlan 2 unsolicited-report-interval 0) or use only **ipv6 multicast vlan** *vid* **unsolicited-report-interval** (e.g., 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 6.6.1; 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
   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 6450, 6350

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 (i.e., 90 seconds) value on the system if no VLAN is specified, use **ipv6 multicast router-timeout** followed by the value 0 (e.g., ipv6 multicast router-timeout 0) or use only **ipv6 multicast router-timeout** (e.g., ipv6 multicast router-timeout).
- To restore the MLD router timeout to its default (i.e., 90 seconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **router-timeout** followed by the value 0 (e.g., ipv6 multicast vlan 2 router-timeout 0) or use only **ipv6 multicast vlan** *vid* **router-timeout** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., 30 seconds) value on the system if no VLAN is specified, use **ipv6 multicast source-timeout** followed by the value 0 (e.g., ipv6 multicast source-timeout 0) or use only **ipv6 multicast source-timeout** (e.g., ipv6 multicast source-timeout).
- To restore the MLD router timeout to its default (i.e., 30 seconds) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **source-timeout** followed by the value 0 (e.g., ipv6 multicast vlan 2 source-timeout 0) or use only **ipv6 multicast vlan** *vid* **source-timeout** (e.g., 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 6.6.1; 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}]**

no ipv6 multicast [vlan *vid***] querying**

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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove an MLD querying entry on the specified VLAN or on the system and return to its default behavior.
- 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 (i.e., disabled) setting on the system if no VLAN is specified, by using only **ipv6 multicast querying** (e.g., ipv6 multicast querying).
- You can also restore the MLD querying to its default (i.e., disabled) setting on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **querying** (e.g., 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
-> no ipv6 multicast vlan 2 querying
```

Release History

Release 6.6.1; 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
   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 6450, 6350

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 (i.e., 2) value on the system if no VLAN is specified, use **ipv6 multicast robustness** followed by the value 0 (e.g., ipv6 multicast robustness 0) or use only **ipv6 multicast robustness** (e.g., ipv6 multicast robustness).
- To restore the MLD robustness variable to its default (i.e., 2) value on the specified VLAN, use **ipv6 multicast vlan** *vid* **robustness** followed by the value 0 (e.g., ipv6 multicast vlan 2 robustness 0) or use only **ipv6 multicast vlan** *vid* **robustness** (e.g., 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 6.6.1; 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}]**

no ipv6 multicast [vlan *vid***] spoofing**

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 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove an MLD spoofing entry on the specified VLAN or on the system and return to its default behavior.
- 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 (i.e., disabled) setting on the system if no VLAN is specified, by using only **ipv6 multicast spoofing** (i.e., ipv6 multicast spoofing).
- You can also restore the MLD spoofing to its default (i.e., disabled) setting on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **spoofing** (i.e., 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
-> no ipv6 multicast vlan 2 spoofing
```

Release History

Release 6.6.1; 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
   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 6450, 6350

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 (i.e., disabled) setting on the system if no VLAN is specified, by using only **ipv6 multicast zapping** (e.g., ipv6 multicast zapping).
- You can also restore the MLD zapping to its default (i.e., disabled) setting on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **zapping** (e.g., 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 6.6.1; 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 6450, 6350

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 (i.e., disabled) setting on the system if no VLAN is specified, by using only **ipv6 multicast proxying** (e.g., ipv6 multicast proxying).
- You can also restore the MLD proxying to its default (i.e., disabled) setting on the specified VLAN, by using only **ipv6 multicast vlan** *vid* **proxying** (e.g., 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 6.6.1; 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
   alaMldProxying
alaMldVlan
   alaMldVlanProxying
```

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 6450, 6350

Usage Guidelines

Specify a VLAN ID to display the configuration information for an individual VLAN.

Examples

```
-> show ip multicast
Status                                          = enabled,
Querying                                        = enabled,
Proxying                                        = disabled,
Spoofing                                        = disabled,
Zapping                                         = disabled,
Querier Forwarding                              = enabled,
Star-G-mode                                     = disabled,
Flood Unknown                                   = disabled,
Dynamic control drop-all status                 = disabled,
Static-neighbor fast-convergence                = 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
```

```
-> show ip multicast vlan 10
Status                                          = enabled,
Querying                                        = enabled,
Proxying                                        = disabled,
Spoofing                                        = disabled,
Zapping                                         = disabled,
Querier Forwarding                              = enabled,
Star-G-mode                                     = 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 47-3.
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 47-38.
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 47-46.
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 47-42.
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 47-44.
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 47-9.
Star-G-mode	Displays the star-G mode status on the interface.
Flood Unknown	Displays if flooding of new multicast packets until the multicast group membership table is updated is enabled or disabled.

output definitions

Dynamic control drop-all status	Displays the dynamic control drop-all status of the IPV4 protocol packets on the switch. You can enable or disable the dynamic control drop-all status with the **ip multicast dynamic-control drop-all status** command, which is described on page 47-5.
Static-neighbor fast-convergence	Displays if IGMP static neighbor fast learning is enabled or disabled.
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.
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 47-26.
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 47-30.
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 47-28.
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 47-32.
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 47-34.
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 47-36.
Max-group	The maximum group count allowed on the port/VLAN.
Max-group action	Displays the maximum group action configured.

Release History

Release 6.6.1; command was introduced.
Release 6.6.5; **Dynamic control drop-all status** output field added.
Release 6.7.2.R04; **Star-G-mode** 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 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.
ip multicast flood-unknown	Enables or disables the processing of IPV4 protocol packets through the CPU.
ip multicast star-g-mode status	Enable or disable star-G mode (*, G) for IPv4 multicast switching.
ip multicast vlan star-g-mode status	Enable or disable star-G mode (*, G) for IPv4 multicast switching on a specific VLAN.

MIB Objects

```
alaIgmp
   alaIgmpStatus
   alaIgmpQuerying
   alaIgmpProxying
   alaIgmpSpoofing
   alaIgmpZapping
   alaIgmpQuerierForwarding
   alaDynamicControlIpv4Status
   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 (e.g. 3/1 specifies port 1 on slot 3)).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Specify a slot and port number to display the configuration information for a specific switch port.

Examples

```
-> show ip multicast port

Total 5 Port-Vlan Pairs

  Port    VLAN       Current Igmp   Max-group   Action
                     Groups
-------+---------+-------------+--------------+---------
    1/1    10             1        1            drop
    1/1    20             1        1            drop
    1/3    15             2        5            replace
    1/4    20             3       10            drop
    1/6    15             5        0            none

-> show ip multicast port 1/1
Max-group 0 Action none
Total 2 Port-Vlan Pairs

  Port    vlan    current IGMP   max-group   action
                   group
-------+-----+-------------+----------+---------
    1/1    10             1        1   drop
    1/1    20             2        5   replace
```

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.

output definitions

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 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ip multicast forward
                                                  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   -
230.0.1.1       0.0.0.0         0.0.0.0          20   *      20   2/11  -

-> show ip multicast forward 230.0.1.1
Total 1 Forwards

* Denotes L2 (*, G) mode
                                                  Ingress     Egress
Group Address   Host Address    Tunnel Address  VLAN  Port  VLAN  Port  RVLAN
---------------+---------------+---------------+-----+-----+-----+-----+------
230.0.1.1       0.0.0.0         0.0.0.0          20   *      20   1/15  -

                                                  Ingress     Egress
Group Address   Host Address    Tunnel Address  VLAN  Port  VLAN  Port  RVLAN
---------------+---------------+---------------+-----+-----+-----+-----+------
255.0.0.1      0.0.0.0         0.0.0.0          10   *    10   2/11  -
```

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. **Note**: 0.0.0.0 in source host field indicates star-G (*, G) mode. In the example, it indicates that star-G mode is enabled on the VLAN 20 for the multicast group address 230.0.1.1.
Tunnel Address	IP source tunnel address of the IP multicast forward.
VLAN	VLAN associated with the IP multicast forward.
Port	The slot and port number of the IP multicast forward. **Note**: * in the source port (ingress) indicates star-G (*, G) mode.
RVLAN	Displays the receiver VLAN association with the receiver port.

Release History

Release 6.6.1; command was introduced.

Related Commands

ip multicast static-group	Creates a static IGMP group entry on a specified port on a specified VLAN.
ip multicast star-g-mode status	Enable or disable star-G mode (*, G) for IPv4 multicast switching.
ip multicast vlan star-g-mode status	Enable or disable star-G mode (*, G) for IPv4 multicast switching on a specific 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ip multicast neighbor

Total 2 Neighbors
Host Address    VLAN  Port  Static  Count  Life
---------------+-----+-----+-------+------+-----
1.0.0.2         1     2/1   no      1      86
0.0.0.0         1     2/13  yes     0      0
```

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.
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 6.6.1; command was introduced.

Related Commands

ip multicast max-group	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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ip multicast querier

Total 2 Queriers
Host Address    VLAN  Port  Static  Count  Life
---------------+-----+-----+-------+------+-----
1.0.0.2         1     2/1   no      1      250
0.0.0.0         1     2/13  yes     0      0
```

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.
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 6.6.1; command was introduced.

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.

show ip multicast group [*ip_address***]**

Syntax Definitions

ip_address	IP multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ip multicast group
Total 1 Groups
* Denotes IPMVLAN
Group Address   Source Address  VLAN  Port   Mode     Static  Count  Life  RVLAN
--------------+---------------+-----+-----+--------+-------+------+-----+------
225.0.0.1       0.0.0.0         *11   1/23  exclude     no      37     259   12
```

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.
Mode	IGMP source filter mode.
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 port.

Release History

Release 6.6.1; command was introduced

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 6450, 6350

Usage Guidelines

If a multicast source packet is sent and stopped, the entry will be removed from the 'show ip multicast source' command immediately.

Examples

```
-> show ip multicast source

Total 1 Sources
Group Address   Host Address    Tunnel Address  VLAN  Port
---------------+---------------+---------------+-----+-----
228.0.0.1       1.0.0.2         0.0.0.0         1     2/1

-> show ip multicast source 230.0.1.1
Total 1 Sources
* Denotes L2 (*, G) mode
Group Address   Host Address    Tunnel Address  VLAN  Port
---------------+---------------+---------------+-----+-----
230.0.1.1       0.0.0.0         0.0.0.0          20   *
```

output definitions

Group Address	IP group address of the IP multicast source.
Host Address	IP host address of the IP multicast source. **Note**: 0.0.0.0 in source host field indicates star-G (*, G) mode. In the example, it indicates that star-G mode is enabled on the VLAN 20 for the multicast group address 230.0.1.1.
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. **Note**: * in the source port indicates star-G (*, G) mode.

Release History

Release 6.6.1; command was introduced.

Related Commands

ip multicast static-group	Creates a static IGMP group entry on a specified port on a specified VLAN.
ip multicast star-g-mode status	Enable or disable star-G mode (*, G) for IPv4 multicast switching.
ip multicast vlan star-g-mode status	Enable or disable star-G mode (*, G) for IPv4 multicast switching on a specific VLAN.

MIB Objects

```
alaIgmpSourceTable
   alaIgmpSourceVlan
   alaIgmpSourceIfIndex
   alaIgmpSourceGroupAddress
   alaIgmpSourceHostAddress
   alaIgmpSourceDestAddress
   alaIgmpSourceOrigAddress
   alaIgmpSourceType
   alaIgmpSourceUpTime
```

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

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast

Status                                          = disabled,
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                                       = 0,
Max-group action                                = none
```

```
-> show ipv6 multicast vlan 1003

Status                                          = enabled,
Querying                                        = enabled,
Proxying                                        = disabled,
Spoofing                                        = disabled,
Zapping                                         = disabled,
Querier Forwarding                              = enabled,
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                                       = 0,
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 **ipv6 multicast status** command, which is described on page 47-52
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 47-82
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 47-90
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 47-42
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 47-88
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 47-54.
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 47-70.

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 47-74.
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 47-72.
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 47-76.
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 47-78
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 47-80
Max-group	The maximum group count allowed on the port/VLAN.
Max-group action	Displays the maximum group action configured.

Release History

Release 6.6.1; command was introduced.

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
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 (e.g. 3/1 specifies port 1 on slot 3)).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6450, 6350

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 ff05:1::5
                                                 Ingress    Egress
Group Address   Host Address    Tunnel Address  VLAN  Port  VLAN  Port
--------------- +---------------+---------------+-----+-----+-----+------
ff05::6 4        444::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 6.6.1; 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

ipv6 multicast max-group	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 6450, 6350

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 6.6.1; 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 6450, 6350

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.

Release History

Release 6.6.1; 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

```
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 6450, 6350

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 ff05:1::5

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 6.6.1; 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
```

48 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 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** **vlan svlan port translate ipmvlan** **show vlan ipmvlan c-tag** **show vlan ipmvlan address** **show vlan ipmvlan port-config** **show ipmvlan port-config** **show vlan ipmvlan port-binding**

vlan ipmvlan

Creates an IP Multicast VLAN.

vlan ipmvlan *ipmvlan-id* **[{enable | disable} | [{1x1 | flat} stp {enable | disable}]] [name** *name-string***] [svlan]**

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 VLAN”).
svlan	Tags the IPMVLAN to be used in VLAN Stacking environment.
ipmvlan-id2	Th last IPMVLAN number in a range of IPMVLANs that you want to configure.

Defaults

parameter	default
enable | disable	**enable**

Platforms Supported

OmniSwitch 6450, 6350

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.
- Use the **svlan** parameter to specify that the IPMVLAN should be used in the VLAN Stacking environment.
- 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 1033 name "multicast vlan" svlan
-> vlan ipmvlan 1333 1x1 stp enable name "multicast vlan" svlan
-> no vlan ipmvlan 1003
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show vlan ipmvlan	Displays IPMVLAN information for a specific IPMVLAN or all IPMVLANs.
show vlan	Displays a list of VLANs and their types configured on the switch.

MIB Objects

```
vlanTable
   vlanNumber
   vlanDescription
   vlanTraffictype
   vlanAdmStatus
   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 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 6450

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 6.6.1; 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, IPv6 address, or a range of addresses to an existing IPMVLAN.

vlan ipmvlan *ipmvlan-id* **address {***ip_address* **|** *ipv6_address* **|** *ipaddress1-ipaddress2* **|** *ipv6address1-ipv6address2***}**

no vlan ipmvlan *ipmvlan-id* **address {***ip_address* **|** *ipv6_address* **|** *ipaddress1-ipaddress2* **|** *ipv6address1-ipv6address2***}**

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 IPM-VLAN.
ipv6_address	Specifies a 128-bit IPv6 Multicast address that will be assigned to the IPMVLAN.
ipaddress1-ipaddress2	Specifies the IP Multicast address range.
ipv6address1-ipv6address2	Specifies the IPv6 Multicast address range.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to disassociate the already assigned IP or IPv6 address from the IPMV.
- If the address is already assigned to another IPMVLAN, the configuration request will fail.
- If you assign a range of addresses to an IPMVLAN, an error message will be displayed for the addresses already assigned to the IPMVLAN.
- A maximum of 128 addresses can be specified in a range. If the range is exceeded, configuration for all the addresses in that range will fail.

Examples

```
-> vlan ipmvlan 1003 address 225.0.0.1
-> vlan ipmvlan 1033 address ff08::3
-> no vlan ipmvlan 1003 address 225.0.0.1
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show vlan ipmvlan address	Displays the IPv4 and IPv6 addresses assigned to single IP Multicast VLAN or all the configured IP Multicast VLANs.

MIB Objects

```
alaipmvVlanIpAddrTable
   alaipmvVlanIpAddrVlanNumber
   alaipmvVlanIpAddrType
   alaipmvVlanIpAddress
   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 6450, 6350

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:

```
-> vlan svlan 1/49 network-port
-> vlan ipmvlan 1033 sender-port port 1/49
```

The following command removes the port configured as sender port:

```
-> no vlan ipmvlan 1003 sender-port port 1/50
```

Release History

Release 6.6.1; command was introduced.

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.

vlan ipmvlan *ipmvlan-id* **receiver-port {port** *slot/port***[**-*port2***]** | **linkagg** *agg_num* **[**-*agg_num2***]} [***receiver vlan-id***]**

no vlan ipmvlan *ipmvlan-id* **receiver-port {port** *slot/port***[**-*port2***]** | **linkagg** *agg_num* **[**-*agg_num2***]} [***receiver vlan-id***]**

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-id	Specifies the receiver vlan to be associated with the receiver ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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. An IPMVLAN can contain multiple receiver ports.
- In the Enterprise mode, the configuration fails if the port configured as a receiver 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 receiver port is not a VLAN Stacking port (user port).

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:

```
-> vlan svlan port 1/1 user-customer-port default-svlan 10
-> vlan ipmvlan 1002 receiver-port port 1/1
-> no vlan ipmvlan 1002 receiver-port port 1/1
```

Release History

Release 6.6.3; command was 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

```
alaipmvReceiverVlanPortTable
   alaipmvReceiverVlanPortIPMVlanNumber
   alaipmvReceiverVlanPortNumber
   alaipmvReceiverVlanPortRcvrVlanNumber
   alaipmvReceiverVlanPortRowStatus
```

vlan svlan port translate ipmvlan

Creates an association between IP Multicast VLAN and customer VLAN (c-tag) on the receiver ports.

vlan svlan port {*slot/port* **|** *agg_num***} translate cvlan** *customer-vlan-id* **{ipmvlan** *ipmvlan-id* **| svlan** *svlan-id***}**

vlan svlan port {*slot/port* **|** *agg_num***} cvlan** *customer-vlan-id* **no ipmvlan** *ipmvlan-id*

Syntax Definitions

slot/port	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 to associate SVLAN / IPMVLAN to a customer VLAN on the receiver port. The valid range is 0–31.
customer-vlan-id	Customer VLAN ID associated with the SVLAN / IPMVLAN.
ipmvlan-id	Specifies the IP Multicast VLAN number. The valid range is 2–4094.
svlan-id	Specifies the SVLAN number identifying the instance.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Use the **no** form of this command to delete the association between SVLAN / IPMVLAN and customer VLAN.
- If the SVLAN / IPMVLAN does not exist, the port is not a VLAN Stacking port, the port is a member of an aggregate, or the aggregate does not exist, then an error message will be displayed.

Examples

```
-> vlan svlan port 1/1 user-customer-port default-svlan 10
-> vlan ipmvlan 1002 receiver-port port 1/1
-> vlan svlan port 1/1 translate cvlan 10 ipmvlan 1002
-> vlan svlan port 1/1 cvlan 10 no ipmvlan 1002
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show vlan ipmvlan port-binding	Displays the translation bindings of an IP Multicast VLAN on a port, an aggregate of ports, or all the ports.

MIB Objects

```
alaVstkSvlanPortTable
   alaVstkSvlanPortNumber
   alaVstkSvlanPortSvlanNumber
   alaVstkSvlanPortCvlanNumber
   alaVstkSvlanPortMode
   alaVstkSvlanPortRowStatus
```

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 6450

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 6.6.1; 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 and IPv6 addresses assigned to a single IP Multicast VLAN or all the configured IP Multicast VLANs.

show vlan ipmvlan [*ipmvlan-id***] address**

Syntax Definitions

ipmvlan-id	Specifies the IP Multicast VLAN number. The valid range is 2–4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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
ffae::1    Ipv6
ffae::2    Ipv6
ffae::3    Ipv6
```

output definitions

IPAddresses	The IP address assigned to IPMVLAN 10.
IPAddresses Type	The IP address type assigned to IPMVLAN 10.

```
-> show vlan ipmvlan address

   ipmvlan    ipAddress    ipAddressType
+---------+------------+------------------+
      100        224.1.2.3        Ipv4
      100        225.1.1.1        Ipv4
      100        ff08::3          Ipv6
      200        224.1.1.2        Ipv4
      200        ff09::1          Ipv6
```

output definitions

ipmvlan	The IPMVLAN ID.
ipAddress	The IP address assigned to the IPMVLAN.
ipAddressType	The IP address type (**IPv4** or **IPv6**).

Release History

Release 6.6.1; command was introduced.

Related Commands

vlan ipmvlan address	Assigns an IPv4 address, IPv6 address, or a range of addresses to an existing IPMVLAN.

MIB Objects

```
alaipmvVlanIpAddrTable
   alaipmvVlanIpAddrVlanNumber
   alaipmvVlanIpAddrType
   alaipmvVlanIpAddress
```

show vlan ipmvlan port-config

Displays the sender and receiver ports 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show vlan ipmvlan port-config
ipmvlan    port        type        RVLAN
----------+-----------+-----------+-------------
100        1/1         sender        -
100        1/2         receiver     10
100        1/3         receiver     20
200        1/10        sender       -
200        1/2         receiver     10
200        1/3         receiver     20

-> show vlan ipmvlan 101 port-config
port       type         RVLAN
---------+------------+--------------
1/11       receiver       10
1/11       receiver       20
1/2        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	The receiver VLAN

Release History

Release 6.6.1; command was introduced.

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
   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 6450, 6350

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 6.6.1; command was introduced.

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
```

show vlan ipmvlan port-binding

Displays the translation bindings of an IP Multicast VLAN on a port, an aggregate of ports, or all the ports.

show vlan ipmvlan port-binding [*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

By default all the IPMVLANs will be displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Use the *slot/port* or *agg_num* parameter with this command to view the IPMVLANs associated with a specific port or an aggregate of ports.

Examples

```
-> show vlan ipmvlan port-binding
  port       ipmvlan     cvlan        type
+---------+-----------+----------+-------------+
  2/2        100          10        receiver
  2/2        100          11        receiver
  0/2         51         151        receiver

-> show vlan ipmvlan port-binding 2/2
  ipmvlan    cvlan        type
+---------+-----------+------------+
   100         10        receiver
   100         11        receiver

-> show vlan ipmvlan port-binding 2
  ipmvlan    cvlan        type
+---------+-----------+------------+
    51        151        receiver
```

output definitions

port	The slot number/physical port number on that module.
ipmvlan	The numerical IPMVLAN ID.

output definitions (continued)

cvlan	The numerical CVLAN ID associated with the IPMV.
type	The type (**sender** or **receiver**) of the IPMVLAN port.

Release History

Release 6.6.1; command was introduced.

Related Commands

vlan svlan port translate ipmvlan	Creates an association between IP Multicast VLAN and customer VLAN (c-tag) on the receiver ports.

MIB Objects

```
alaipmvVlanPortTable
   alaipmvVlanPortIPMVlanNumber
   alaipmvVlanPortPortNumber
   alaipmvVlanPortPortType
```

49 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 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 can be stored locally in the switch user database.
- Local user database. User information can be configured for Authenticated Switch Access. For functional management access, users can be allowed to access specific command families or domains. Alternately, users can 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

A summary of the available commands is listed here:

Authentication servers	**aaa radius-server** **aaa test-radius-server** **aaa radius-health-check** **aaa tacacs+-server** **aaa tacacs command-authorization** **aaa tacacs server-wait-time** **aaa ldap-server** **aaa ace-server clear** **aaa classification-rule mac-address** **aaa radius nas-identifier** **aaa radius nas-ip-address** **show aaa radius config** **show aaa radius-health-check config**
Authenticated Switch Access	**aaa authentication** **aaa authentication default** **aaa accounting mac** **aaa accounting session** **aaa accounting command** **show aaa server** **show aaa radius-health-check config** **show radius-server statistics** **clear radius-server statistics** **show aaa authentication 802.1x** **show aaa accounting mac** **show aaa accounting**

Authenticated Switch Access - Enhanced Mode	**aaa switch-access mode** **aaa switch-access ip-lockout-threshold** **aaa switch-access banned-ip release** **aaa switch-access priv-mask** **aaa switch-access management-stations** **aaa switch-access management-stations ip-address** **show aaa switch-access mode** **show aaa switch-access ip-lockout-threshold** **show aaa switch-access banned-ip** **show aaa switch-access priv-mask** **show aaa switch-access management-stations**
802.1X Port-Based Network Access Control	**aaa authentication 802.1x** **aaa authentication mac** **aaa accounting 802.1x** **show aaa authentication mac** **show aaa accounting 802.1x**
Local User Database and Partitioned Management	**user** **password** **user password-size min** **user password-expiration** **show user** **show aaa classification-rule**
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** **debug command-info** **debug end-user profile**
Administrative User Logout	**aaa admin-logout**

Common Criteria	**system common-criteria** **show system common-criteria** **aaa certificate update-ca-certificate** **aaa certificate update-crl** **aaa certificate generate-rsa-key key-file** **aaa certificate generate-self-signed** **aaa certificate view** **aaa certificate delete** **aaa certificate generate-csr**
End-user Profiles	**user** **aaa admin-logout** **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** **aaa classification-rule lldp med-endpoint** **show aaa user-network-profile** **show aaa classification-rule**
Host Integrity Check	**aaa byod white-list** **aaa hic allowed-name** **aaa hic** **aaa hic web-agent-url** **aaa hic custom-proxy-port** **aaa hic redundancy background-poll-interval** **aaa hic server-failure mode** **aaa hic server-failure policy user-network-profile change** **show aaa hic** **show aaa hic host** **show aaa hic server** **show aaa hic allowed** **show aaa hic server-failure policy**
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** **show aaa priv hexa**

BYOD commands	**aaa redirect-server** **aaa redirect url** **aaa port-bounce** **aaa redirect pause-timer** **aaa redirect proxy-server-port** **aaa user-network-profile** **aaa byod white-list** **aaa byod white-list no** **show aaa redirect-server** **show aaa redirect url-list** **show aaa port-bounce status** **show aaa redirect pause-timer** **show byod host** **show byod status** **show byod status** **show aaa user-network-profile**
Zero Configuration MDNS and SSDP Relay Commands	**mdns-relay (**deprecated) **mdns-relay tunnel (**deprecated) **show mdns-relay config (**deprecated) **zeroconf mdns admin-state** **zeroconf ssdp admin-state** **zeroconf mode** **zeroconf responder-ip** **zeroconf gateway-vlan-list** **zeroconf access-vlan-list** **show zeroconf config**

aaa radius-server

Configures or modifies a RADIUS server for Authenticated Switch Access or 802.1X port access control. This command is used to configure NAS server configurations for the RADIUS server, enable or disable unique session ID for RADIUS accounting.

aaa radius-server *server* **host {***hostname* | *ip_address***} [***hostname2* | *ip_address2***] {key** *secret* | **hash-key** *hash_secret*|| **prompt-key} [salt** *salt* | **hash-salt** *hash_salt***] [retransmit** *retries***] [timeout** *seconds***] [auth-port** *auth_port***] [acct-port** *acct_port***] [mac-address-format-status {enable | disable} mac-address-format {uppercase | lowercase}] [nas-port {default | ifindex} | nas-port-id {enable | disable}] nas-port-type [xdsl | x75x25 | x25 | wireless-other | wireless-ieee-802-11 | virtual | sync | sdsl-symmetric-dsl | piafs | isdn-sync | isdn-async-v120 | isdn-async-v110 | idsl | hdlc-clear-channel | g3-fax | Ether-net | cable | async | adsl-dmt | adsl-cap-asymmetric-dsl] [unique-acct-session-id {enable | disable}]**

no aaa radius server *server*

Syntax Definitions

server	The name of the RADIUS server.
hostname	The host name (DNS name) of the primary RADIUS server. The host name or IP address is required when creating a server.
ip_address	The IP address of the primary RADIUS server. An IP address or host name is required when creating a server.
hostname2	The host name (DNS name) of an optional backup RADIUS server.
ip_address2	The IP address of an optional backup RADIUS server.
secret	The shared secret known to the switch and the server, but which is not sent over the network. Can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case sensitive.
hash_secret	A shared secret for which the input must be in an encrypted format. The maximum length of the hash-key is 128 characters.
prompt-key	This option allows to enter the secret key in a masked format rather than as clear text. When this option is selected, press the Enter key. A prompt appears prompting to enter the secret key. Secret key needs to be re-entered, and only if both the entries match, command is accepted. Key provided in this mode is not displayed on the CLI as text.
salt	The input given through ‘salt’ will be used to add randomness to the encryption of key. The maximum length of the salt is 64 characters, and must be in clear text format. By default, system time (24-hour value format) will be taken as default salt value.
hash_salt	The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt is 160 characters.
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.
mac-address-format-status	enable: Enables case-sensitive MAC address authentication. disable: Disables case-sensitive MAC address authentication.
uppercase	Specifies that the MAC address format and other IDs sent to RADIUS server will be in uppercase.
lowercase	Specifies that the MAC address format and other IDs sent to RADIUS server will be in lowercase.
nas-port	Physical port of the NAS server. **default**: When NAS port is configured as **default**, access request/accounting request packet will be sent with NAS port value as 77. **ifindex:** When NAS port is configured as **ifindex,** authenticating port will be converted to ifIndex (slot*1000+port) and will be sent using the NAS port attribute.
nas-port-id	The interface identifier of the NAS port authenticating the user. **enable**: Enable NAS port-ID attribute. When enabled, authenticating port will be converted to ifIndex (slot*1000+port) and will be sent using NAS port ID attribute. **disable**: Disable NAS port-ID attribute.
nas-port-type	Type of the physical port of the NAS server that is authenticating the user. The various options available are **x75, x25, xdsl, wireless-other, wireless-ieee-802-11, virtual, sync, sdsl-symmetric-dsl, piafs, isdn-sync, isdn-async-v120, isdn-async-v110, idsl, hdlc-clear-channel, g3-fax, Ethernet, cable, async, adsl-dmt, adsl-cap-asymmetric-dsl**.
unique-acct-session-id	**enable**: Enable unique session ID for RADIUS accounting. **disable**: Disable unique session ID for RADIUS accounting.

Defaults

parameter	default
retries	3
seconds	2
auth_port	1812
acct_port	1813
mac-address-format-status enable | disable	disable
mac-address-format uppercase | lowercase	uppercase
nas-port	default
nas-port-id	disable
nas-port-type	Ethernet
unique-acct-session-id	disable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to remove a RADIUS server from the configuration. Only one server can be deleted at a time.
- A host name (or IP address) and a secret key are required when configuring a server.
- If ‘key’ and ‘hash-key’ parameters are configured at a time, hash-key value is given priority over key.
- The user configured or default salt along with the server name will be combined with 'key' and encrypted as a whole, the output of which will be displayed under ‘hash-key'.
- If ‘salt’ and ‘hash-salt’ parameters are configured at a time, hash-salt value is given priority over salt.
- The special character '!' and pure integers will not be accepted as a valid input for both salt and hash-salt.
- The input given through ‘salt’ and ‘hash-salt’ is encrypted and will be displayed as ‘hash-salt’ in 'show configuration snapshot' command.
- Backward compatibility for ‘salt’ and ‘hash-salt’ is not supported. In case of an accidental downgrade, boot.cfg error is generated for that particular configuration, and re-configuration is required.
- The primary server and the backup server must both be RADIUS servers.
- The case sensitive **mac-address-format** can be applied only when **mac-address-format-status** is enabled.
- The MAC address is sent as part of Radius packets, the following data is sent as lowercase when MAC address format is selected as lowercase using the **mac-address-format lowercase** keywords:
  - user-name and password, in Access-Request and Accounting-Request
  - Calling-Station-ID in Access-Request packet.
- When **mac-address-format-status** is not applied or disabled, by default the related RADIUS packet data is sent in uppercase format.
- NAS port configuration is supported for supplicant or non-supplicant clients, and ASA users (management sessions) like FTP, telnet, HTTP, console, HTTPS, and SSH.
- Authentication and accounting server must be configured as RADIUS for 802.1x supplicant clients, non-supplicant clients, and ASA users prior to NAS port configuration.
- NAS port and NAS port ID configurations are mutually exclusive. Either NAS port or NAS port ID can be configured at a time for the RADIUS server. For more information on the configuration behavior, refer to “Managing Authentication Servers” chapter in *OmniSwitch AOS Release 6 Network Configuration Guide*.
- **show configuration snapshot aaa** command displays the value of NAS port, NAS port ID, and NAS port type configured for the RADIUS server. However, NAS port configuration will not be displayed when these attributes are configured with default values.
- RADIUS Accounting Session ID feature maintains a unique session ID in RADIUS accounting for 802.1x supplicant or non-supplicant clients, captive portal users, and management sessions like FTP, telnet, HTTP, console, HTTPS, and SSH.
- Authentication server and accounting server must be configured as RADIUS server for 802.1x supplicant clients, 802.1x non-supplicant clients, captive portal users, and management users prior to unique session ID configuration.

- Use **show configuration snapshot aaa** and **show aaa server** commands to view the unique session ID configuration.
- It is recommended that Radius Health Check is enabled on all the radius server configured for 802.1x and MAC-authentication in the system. This improves the time in which the 802.1x users are authenticated. Use the **aaa radius-health-check** command to configure Radius Health Check. **show aaa server** command displays the reachability status of all the configured RADIUS servers configured on the switch.

Examples

```
-> aaa radius-server "Server1" host 10.10.2.1 key wwwtoe timeout 5
-> no aaa radius-server "Server1"

-> aaa radius-server "Server1" host 10.10.2.1 hash-key e47ac0f11e9fa869

-> aaa radius-server "Server1" host 10.10.2.1 key wwwtoe salt random

-> aaa radius-server "Server1" host 10.10.2.1 key wwwtoe hash-salt
c7f5eee2c0f9b33e72e3482673fb6059

-> aaa radius-server "Server1" mac-address-format-status enable mac-address-format
lowercase

-> aaa radius-server "Server1" nas-port-id enable nas-port-type async

-> aaa radius-server "Server1" unique-acct-session-id enable
-> aaa radius-server "Server1" unique-acct-session-id disable

-> aaa radius-server "Server1" prompt-key host 10.10.2.1
Enter key:   *******
Re-enter key: ******
```

Release History

Release 6.6.1; command was introduced.
Release 6.6.4; **mac-address-format-status, mac-address-format, nas-port**, **nas-port-id**, **nas-port-type, unique-acct-session-id** parameters added.
Release 6.7.1.R04; **prompt-key** parameter added.
Release 6.7.2.R03; **hash-key** parameter added.
Release 6.7.2.R06; **salt** and **hash-salt** parameters added.

Related Commands

aaa classification-rule mac-address	Displays information about AAA servers.
aaa authentication	Specifies the AAA servers to be used for Authenticated Switch Access.
aaa authentication 802.1x	Enables/disables the switch for 802.1X authentication. Specifies the RADIUS authentication server used for 802.1X authentication.
aaa authentication mac	Enables/disables the switch for MAC authentication. Specifies the RADIUS authentication server used for MAC authentication.
aaa accounting 802.1x	Enables/disables accounting for 802.1X authentication sessions.
aaa accounting mac	Enables/disables accounting for 802.1X non-supplicant (MAC-based) authentication sessions.
aaa accounting session	Configures an accounting server or servers for authenticated switch sessions.
show aaa server	Displays information about a particular AAA server or AAA servers.

MIB Objects

```
aaaServerTable
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasRadKey
   aaasRetries
   aaasTimout
   aaasRadMacAddrCaseStatus
   aaasRadMacAddrFormat
   aaasRadAuthPort
   aaasRadAcctPort
   aaasRadUniqueAcctSessionId
   aaasRadKeyHash
   aaasRadSalt
   aaasRadSaltHash
```

aaa test-radius-server

Starts the authentication or accounting test for the given username and password. Radius test tool allows you to test the radius server reach ability from the switch and validate the authentication/accounting port of the Radius server.

aaa test-radius-server *server-name* **type {authentication user** *user-name* **password** *password* **[method {MD5 | PAP}] | accounting user** *user-name***}**

Syntax Definitions

server-name	Server name for which test has been configured.
authentication | accounting	The type of test to be configured.
user-name	User name for which test has been configured.
password	Password for the given user name.
MD5 | PAP	Password encryption method for the test.

Defaults

By default, the authentication method is MD5.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- RADIUS server configurations like RADIUS server name, acct-port, auth-port, secret key, Retransmit Count, Timeout should be done on the AOS switch before starting the test tool.
- If the server name for the given test is not configured, the command displays an error as “Unknown server”.
- The maximum length of the user name should not exceed 63 characters.
- The length of password should not exceed 128 characters.

Examples

```
-> aaa radius-server abc host “172.21.160.26” auth-port 1812 acct-port 1813 key
"1234"
-> aaa test-radius-server abc type authentication user admin password switch method
MD5 Testing Radius Server <172.21.160.26/abc>

-> aaa test-radius-server abc type authentication user admin password switch method
pap Testing Radius Server <172.21.160.26/abc>

-> aaa test-radius-server abc type accounting user admin
Testing Radius Server <172.21.160.26/abc>

-> aaa test-radius-server abc type authentication user admin password switch
Testing Radius Server <172.21.160.25/abc>
```

```
-> aaa test-radius-server abc type authentication user admin password switch
Testing Radius Server <172.21.160.25/abc>
```

Release History

Release 6.6.3; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access or 802.1X port access control.
aaa authentication	Specifies the AAA servers to be used for Authenticated Switch Access.
show aaa server	Displays information about a particular AAA server or AAA servers.

MIB Objects

N/A

aaa radius-health-check

Configures the radius health check feature for a specific radius server. The feature allows to poll individual radius servers at the specified interval and re-authenticate the users or take action, if the server status is changed to up from down.

aaa radius-health-check name *server-name* **status {enable | disable} polling-interval** *seconds* **user-name** *user-name* **password** *password* **failover {enable | disable}**

no aaa radius-health-check name *server-name*

Syntax Definitions

server-name	The name of the radius server for which radius health check is configured.
status	The status of the radius health check feature for the specified server.
polling-interval	The periodic interval at which the radius server needs to be probed. The valid range is from 20 seconds to 3600 seconds.
username	The username which is used in radius packet to probe the server.
password	Password for the given user name which is used in radius packet to probe the server.
failover	Specify whether action should be taken for timed-out users, if the server changes the operational status from DOWN to UP.

Defaults

parameter	default
status	disable
polling-interval	50
user-name	alcatel
password	alcatel
failover	disable

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- RADIUS server configurations like RADIUS server name, acct-port, auth-port, secret key, Retransmit Count, Timeout should be done on the AOS switch before configuring the radius health check feature.
- If the server name for the radius health check is not configured, the command displays an error as “Unknown server”.
- The maximum length of the user name must not exceed 63 characters.
- The length of password must not exceed 128 characters.

- Use the **no** form of the command to remove the radius health check configuration from the radius server.
- It is recommended that Radius Health Check is enabled on all the radius servers configured for 802.1x and MAC-authentication in the system. This improves the time in which the 802.1x users are authenticated.

Examples

```
-> aaa radius-health-check name rad1 status enable polling-interval 700 username
admin password Password1 failover disable
-> no aaa radius-health-check name rad1
```

Release History

Release 6.7.1 R03; command was introduced.

Related Commands

show aaa radius-health-check config	Displays the radius health check configuration information of radius servers.
show aaa server	Displays information about a particular AAA server or AAA servers.

MIB Objects

```
aaasRadHealthstatus
   aaasRadPollInterval
   aaasRadFailoverStatus
   aaasRadUser
   aaasRadPasswd
```

aaa tacacs+-server

Configures or modifies a TACACS+ server for Authenticated Switch Access.

aaa tacacs+-server *server* **host {***hostname* **|** *ip_address***} [***hostname2* **|** *ip_address2***] [key** *secret* **||** **hash-key** *hash_secret*|| **prompt-key] [salt** *salt* **|** **hash-salt** *hash_salt***] [timeout** *seconds***] [port** *port***]**

no aaa tacacs+-server *server*

Syntax Definitions

server	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.
hash_secret	A shared secret for which the input must be in an encrypted format. The maximum length of the hash-key is 128 characters.
salt	The input given through ‘salt’ will be used to add randomness to the encryption of key. The maximum length of the salt is 64 characters, and clear text format. By default, system time (24-hour value format) will be taken as default salt value.
hash_salt	The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt is 160 characters.
prompt-key	This option allows to enter the secret key in a masked format rather than as clear text. When this option is selected, press the Enter key. A prompt appears prompting to enter the secret key. Secret key needs to be re-entered, and only if both the entries match, command is accepted. Password provided in this mode is not displayed on the CLI as text.
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 6450, 6350

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.
- A host name (or IP address) and a secret are required when configuring a server.
- If ‘key’ and ‘hash-key’ parameters are configured at a time, hash-key value is given priority over key.
- The user configured or default salt along with the server name will be combined with 'key' and encrypted as a whole, the output of which will be displayed under ‘hash-key'.
- If ‘salt’ and ‘hash-salt’ parameters are configured at a time, hash-salt value is given priority over salt.
- The special character '!' will not be accepted as a valid input for both salt and hash-salt.
- The input given through ‘salt’ and ‘hash-salt’ is encrypted and will be displayed as ‘hash-salt’ in 'show configuration snapshot' command.
- Backward compatibility for ‘salt’ and ‘hash-salt’ is not supported. In case of an accidental downgrade, boot.cfg error is generated for that particular configuration, and re-configuration is required.
- 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

-> aaa tacacs+-server tpub host 10.10.2.2 hash-key e47ac0f11e9fa869

-> aaa tacacs+-server tpub host 10.10.2.2 key otna salt random

-> aaa tacacs+-server tpub host 10.10.2.2 key otna hash-salt
c7f5eee2c0f9b33e72e3482673fb6059

-> aaa tacacs+-server tpub prompt-key host 10.10.2.2
Enter key:   *******
Re-enter key: *******
```

Release History

Release 6.6.1; command was introduced.
Release 6.7.1.R04; **prompt-key** parameter added.
Release 6.7.2.R06; **salt** and **hash-salt** parameters added.

Related Commands

aaa classification-rule mac-address	Displays information about AAA servers.
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 Switch Access.

MIB Objects

```
aaaServerTable
   aaasName
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasTacacsKey
   aaasTimout
   aaasTacacsPort
   aaasTacacsSalt
   aaasTacacsSaltHash
```

aaa tacacs command-authorization

Configures a command based authorization in TACACS+ server, for authenticated switch.

aaa tacacs command-authorization {enable | disable}

Syntax Definitions

enable	Enable command based authorization in TACACS+ server
disable	Disable command based authorization. This enables partition-management family based authorization in TACACS+ server.

Defaults

parameter	default
enable | disable	**disable**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command is applicable only for CLI commands.
- If this command is enabled, then in the TACACS+ server the authorization of every command executed on the switch is command based. CLI commands executed on the switch are sent for authorization to the TACACS+ server along with-mode of operation (read or read-write). After authorization, the server will send the response message to the TACACS+ client.
- If the command is disabled, then in the TACACS+ server the authorization is partition-management family based.
- Use **show configuration snapshot aaa** command to view the configuration details of this command.

Examples

```
-> aaa tacacs command-authorization enable
-> aaa tacacs command-authorization disable
```

Release History

Release 6.6.5; command was introduced.

Related Commands

show aaa server	Displays information about a particular AAA server or AAA servers.

MIB Objects

```
aaaTacacsServerCmdAuthorization
```

aaa tacacs server-wait-time

Configures the wait time of TACACS+ server during command authorization process.

aaa tacacs server-wait-time *num*

Syntax Definitions

num	The wait time of the TACACS+ server. The range is 0 to 200 seconds.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> aaa tacacs server-wait-time 4
```

Release History

Release 6.6.5; command was introduced.

Related Commands

show aaa server	Displays information about a particular AAA server or AAA servers.

MIB Objects

```
aaaTacacsServerWaitTime
```

aaa ldap-server

Configures or modifies an LDAP server for Authenticated Switch Access.

aaa ldap-server *server_name* **host {***hostname* | *ip_address***} [{***hostname2* | *ip_address2*}**] dn** *dn_name* **{password** *super_password* | **hash-password** *hash_super_password* | **prompt-password} [salt** *salt* | **hash-salt** *hash_salt***] base** *search_base* **[retransmit** *retries***] [timeout** *seconds***] [ssl | no ssl] [port** *port***]**

no aaa ldap-server *server-name*

Syntax Definitions

server_name	The name of the LDAP server.
hostname	The host name (DNS) of the primary LDAP server. The host name or IP address is required when creating a 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 server.
super_password	The super-user password recognized by the LDAP-enabled directory servers. The password can be clear text or hexadecimal format. Required when creating a server.
hash_super_password	The password for which the input must be in an encrypted format, known only to switch and the server. The maximum length of the hash-password is 160 characters.
prompt-password	This option allows to enter the super-user password in a masked format rather than as clear text. When this option is selected, press the Enter key. A password prompt appears prompting to enter the super-user password. Password needs to be re-entered, and only if both the passwords match, command is accepted. Password provided in this mode is not displayed on the CLI as text.
salt	The input given through ‘salt’ will be used to add randomness to the encryption of password. The maximum length of the salt is 64 characters, and clear text format. By default, system time (24-hour value format) will be taken as default salt value.
hash_salt	The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt is 160 characters.
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 server.
retries	The number of retries the switch makes to the LDAP server to authenticate a user before trying the backup server.

seconds	The timeout in seconds for server replies to authentication requests from the switch.
ssl	Enables a secure switch layer (SSL) between the switch and the LDAP server.
no ssl	Disables a secure switch layer (SSL) between the switch and the LDAP server.
port	The port number for the primary LDAP server and any backup server. Must match the port number configured on the server.

Defaults

Defaults for optional parameters are as follows:

parameter	default
port	389 (SSL disabled) 636 (SSL enabled)
retries	3
seconds	2
ssl | no ssl	**no ssl**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The *dn_name* must be different from the *search_base* name.
- Use the **no** form of the command to remove an LDAP server from the configuration. Only one server may be removed at a time.
- The port number configured on the switch must match the port number configured for the server.
- The user configured or default salt along with the server name will be combined with 'password' and encrypted as a whole, the output of which will be displayed under ‘hash-password'.
- If ‘password’ and ‘hash-password’ parameters are configured at a time, hash-password value is given priority over password.
- The special character '!' will not be accepted as a valid input for both salt and hash-salt.
- The input given through ‘salt’ and ‘hash-salt’ is encrypted and will be displayed as ‘hash-salt’ in 'show configuration snapshot' command.
- Backward compatibility for ‘salt’ and ‘hash-salt’ is not supported. In case of an accidental downgrade, boot.cfg error is generated for that particular configuration, and re-configuration is required.

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
```

```
-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager prompt-password base c=us
retransmit 4
Enter password:*******
Re-enter password:*******

-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager hash-password
c7f5eee2c0f9b33e72e3482673fb6059 base c=us

-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager hash-password
c7f5eee2c0f9b33e72e3482673fb6059 salt random base c=us

-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager hash-password
c7f5eee2c0f9b33e72e3482673fb6059 hash-salt c7f5eee2c0f9b33e72e3482673fb6059 base
c=us
```

Release History

Release 6.6.1; command was introduced.
Release 6.7.1.R04; **prompt-password** parameter added.
Release 6.7.2.R06; **hash-password**, **salt,** and **hash-salt** parameters added.

Related Commands

aaa classification-rule mac-address	Displays information about AAA servers.
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 Switch Access.

MIB Objects

```
aaaServerTable
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasLdapPort
   aaasLdapDn
   aaasLdapPasswd
   aaasLdapSearchBase
   aaasLdapServType
   aaasRetries
   aaasTimeout
   aaasLdapEnableSsl
   aaasLdapSalt
   aaasLdapSaltHash
   aaasLdapPasswdHash
```

aaa ace-server clear

Clears the ACE secret on the switch. An ACE/Server generates “secrets” that it sends to clients for authentication. The secret cannot be configured on the switch but can be cleared on the switch.

aaa ace-server clear

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If the server and the switch gets out of sync, clear the ACE secret on the switch. See ACE/Server documentation in RSA Security 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 6.6.1; command was introduced.

Related Commands

aaa authentication	Specifies servers for Authenticated Switch Access.
aaa classification-rule mac-address	Displays information about AAA servers configured for the switch.

MIB Objects

```
aaaServerTable
   aaasAceClear
```

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} { local |default | ACE} *server1* **[***server2***...]**

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.). 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 can 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 radius-health-check**, 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 4 backups may be specified (including **local**). These backups are only used if *server1* becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.
local	Specifies that the local user database will be a backup for the authentication servers. If you want to use the local user database as the only authentication server, specify **local** for *server1*.

Defaults

- At switch startup, Authenticated Switch Access is available through console port via the local database. Authentication for other management interfaces (Telnet, FTP, etc.) is disabled.
- The default user on the switch is **admin**, and **switch** is the password.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The server type may be RADIUS, TACACS+, LDAP, ACE/Server, or the local user database. Up to 5 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 radius-health-check**, 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.
- Local authentication for session access such as HTTP, FTP, SSH , Telnet and Console access is allowed even before the external server authentication.
- Incase username is not available in local database, then retry to the next authentication server is initiated.
- Session is terminated in case of authentication with incorrect password in local database.
- 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.
- For SNMP and Default sessions, Local cannot be configured as the first authentication method.

Examples

```
-> aaa authentication telnet local server1 server2 server3 server4
-> aaa authentication telnet server1 server2 server3 server4 local
-> no aaa authentication telnet
```

Release History

Release 6.6.1; command was introduced.
Release 6.7.2.R05; Enhancement to allow local authentication even before external server authentication.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for Authenticated Switch Access.
user	Configures user information for the local database on the switch.
aaa classification-rule mac-address	Displays information about servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAuthSATable
   aaatsInterface
   aaasName
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
   aaatsName5
```

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 6450, 6350

Usage Guidelines

Use the **aaa authentication** command to set the default servers.

Examples

```
-> aaa authentication telnet default
-> aaa authentication default default
```

Release History

Release 6.6.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access.
aaa radius-health-check	Configures or modifies an LDAP server for Authenticated Switch Access.
user	Configures user information for the local database on the switch.
aaa classification-rule mac-address	Displays information about servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAuthSATable
   aaatsName1
   aaatsName2
   aaatsName3
   aaatsName4
   aaatsName5
```

aaa authentication 802.1x

Enables/disables the switch for 802.1X authentication.

aaa authentication 802.1x *server1* **[***server2***] [***server3***] [***server4***] [***server5***]**

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...server5	The names of backup servers for authenticating 802.1X users. Up to 4 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 6450, 6350

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 5 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 6.6.1; 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 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
   aaatxName5
   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***] [***server5***]**

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...server5	The names of backup servers used for MAC authentication. Up to 4 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 6450, 6350

Usage Guidelines

- Up to 5 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 6.6.1; 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.
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 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
   aaaMacSrvrName5
```

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 radius-health-check**, and **aaa ldap-server** commands.
server2...	The names of backup servers for 802.1X accounting. Up to 4 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 51, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to disable accounting for 802.1X ports.
- Up to 5 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 radius-health-check**, and **aaa ldap-server** commands.

Examples

```
-> aaa accounting 802.1x rad1 local
-> no aaa accounting 802.1x
```

Release History

Release 6.6.1; 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 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
   aaacxName5
```

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 radius-health-check**, and **aaa ldap-server** commands.
server2...	The names of backup servers for accounting. Up to 4 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 51, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to disable accounting.
- Up to 5 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 radius-health-check**, and **aaa ldap-server** commands.

Examples

```
-> aaa accounting mac rad1 local
-> no aaa accounting mac
```

Release History

Release 6.6.3; 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
   aaaAcctSvr5
   aaaAcctSvrRowStatus
```

aaa accounting session

Configures an accounting server or servers for authenticated switch sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

aaa accounting session *server1* **[***server2***...] [local]**

no accounting session

Syntax Definitions

server1	The name of the RADIUS, 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 radius-health-check**, and **aaa ldap-server** commands.
server2...	The names of backup servers. Up to 4 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 51, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to disable accounting for Authenticated Switch Access.
- Up to 5 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 radius-health-check**, and **aaa ldap-server** commands.

Examples

```
-> aaa accounting session ldap1 radius2 local
-> no aaa accounting session
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show aaa accounting mac	Displays information about accounting servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAcctsaTable
   aaacsName1
   aaacsName2
   aaacsName3
   aaacsName4
   aaacsName5
```

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 radius-health-check** commands.
server2...	The names of TACACS+ backup servers. Up to 4 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 51, "Switch Logging Commands," for information about Switch Logging commands.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of the command to disable command accounting.
- Up to 5 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 radius-health-check** command.

Examples

```
-> aaa accounting command tacacs1 tacacs2 tacacs3
-> no aaa accounting command
```

Release History

Release 6.6.1; command was introduced.

Related Commands

show aaa accounting mac	Displays information about accounting servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAcctCmdTable
   aaacmdSrvName1
   aaacmdSrvName2
   aaacmdSrvName3
   aaacmdSrvName4
   aaacmdSrvName5
```

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* **| password-prompt} [expiration {***day* | *date***}] [read-only | read-write [***families... | domains...***| view** *viewname* **| all | none | all-except** *families...***]] [no snmp | no auth | sha | md5 | sha+des | md5+des | sha+3des | sha+aes | sha+aes192 | sha+aes256 | sha224 | sha224+3des | sha224+aes | sha224+aes192 | sha224+aes256 | sha256 | sha256+3des | sha256+aes | sha256+aes192 | sha256+aes256]] [priv-password** *password* | **prompt-priv-passwd] [console-only {enable | disable}]**

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.
password-prompt	Select this option with the 'user' command to configure the password for the user. When this option is selected, a password prompt appears and the password can be provided. Password needs to be re-entered, and only if both the passwords match, command is accepted. Password provided in this mode is not displayed on the CLI as text.
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.
viewname	Specifies the view name to be integrate with the new or existing user.
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.
all-except	Specifies that functional privileges for families followed by 'all-except' are disabled 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 is used for authenticating SNMP PDU for the user.
md5	Specifies that the MD5 authentication algorithm is used for authenticating SNMP PDU for the user.
sha+des	Specifies that the SHA authentication algorithm and DES encryption standard is used for authenticating and encrypting SNMP PDU for the user.
md5+des	Specifies that the MD5 authentication algorithm and the DES encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha+3des	Specifies that the SHA authentication algorithm and 3DES encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha+aes	Specifies that the SHA authentication algorithm and AES encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha+aes192	Specifies that the SHA authentication algorithm and AES192 encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha+aes256	Specifies that the SHA authentication algorithm and AES256 encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha224	Specifies that the SHA224 authentication algorithm is used for authenticating SNMP PDU for the user.
sha224+3des	Specifies that the SHA224 authentication algorithm and 3DES encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha224+aes	Specifies that the SHA224 authentication algorithm and AES encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha224+aes192	Specifies that the SHA224 authentication algorithm and AES192 encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha224+aes256	Specifies that the SHA224 authentication algorithm and AES256 encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha256	Specifies that the SHA256 authentication algorithm is used for authenticating SNMP PDU for the user.
sha256+3des	Specifies that the SHA256 authentication algorithm and 3DES encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha256+aes	Specifies that the SHA256 authentication algorithm and AES encryption standard is used for authenticating and encrypting SNMP PDU for the user.

sha256+aes192	Specifies that the SHA256 authentication algorithm and AES192 encryption standard is used for authenticating and encrypting SNMP PDU for the user.
sha256+aes256	Specifies that the SHA256 authentication algorithm and AES256 encryption standard is used for authenticating and encrypting SNMP PDU for the user.
priv-password	Separate password that is used for encryption. (8-30 characters)
prompt-priv-passwd	This option allows to enter the privacy password in a masked format rather than as clear text. Select this option with the 'user' command to configure the privacy password for the user. Press the Enter key. A password prompt appears and the privacy password can be provided. Password needs to be re-entered, and only if both the passwords match, command is accepted. Password provided in this mode is not displayed on the CLI as text.
name	The name of an end-user profile associated with this user. Configured through the **aaa admin-logout** command. Cannot be associated with the user if command families/domains are associated with the user.

Defaults

By default, if a user is created without indicating the read and write privileges and SNMP access, the user will be given privileges based on the *default user account*. The default user account may be modified, but by default it has the following privileges:

parameter	default
read-only | read-write	**read-only**

- By default, the password will be encrypted using SHA for all non SNMP users, including admin user.
- For SNMP users without authentication, password will be encrypted with SHA.
- For SNMP users with authentication, it will be encrypted with the authentication method set for the user. If user is created with MD5, then it will be still encrypted with MD5.

For more information about the default user account, see the *OmniSwitch AOS Release 6 Switch Management Guide*.

Platforms Supported

OmniSwitch 6450, 6350

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.)
- SHA2 (SHA224 and SHA256) hashing algorithms can be configured for **admin** user. The default hash algorithm for admin user is SHA1. 'Snmp authentication' field in the **show user** command displays the hashing algorithm configured for the **admin** user.
- The hashing algorithm modification must always be associated with the password change, that is, whenever the **admin** user's hashing algorithm is modified, the admin user's password must be reconfigured (that is new password must be entered).
- If the hashing algorithm is modified to SHA2 for the **admin** user, in case of software downgrade, SNMP access to the admin user will be enabled. To avoid this, configure the hash level of the admin user to 'no snmp' before downgrade using the command **user admin password** <*string*> **no snmp**.
- Either privileges or an end-user profile may be associated with a user; both cannot be configured for the same user.
- New users or updated user settings are saved *automatically*; that is, these settings do not require the **write memory**, **copy running-config working**, or **configuration snapshot** command to save user settings over a reboot.
- The priv-password token is accepted only when SNMP level with encryption is configured for the user. If SNMP level with encryption is not selected and **priv-password** is configured, then CLI command is rejected with error.
- If priv-password is not configured for the user with encryption SNMP level, then user password parameter is used for priv-password (both for authentication/encryption).
- Password policy is not applicable for the new optional parameter **priv-password**.

- For authenticating switch access through other access types such as telnet, FTP, SSH the existing user password will be used irrespective of whether **priv-password** is configured or not.
- When the SNMP level for an existing user with **priv-password** configured is changed from one encryption level to another encryption level, then the previously configured priv-password will not be used with the new SNMP level. Priv-password needs to be configured again when SNMP level is changed for an existing user.

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 ip-routing ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-security	session aaa

Examples

```
-> user techpubs password writer read-only config
-> no user techpubs

-> user techpubs password-prompt
Enter password: *******
Reenter password: ********
```

The following example will configure user ‘admin’ to use sha256 hash.

```
-> user admin password switch123 sha256
```

The following example creates a user with read-write privileges for all families except dshell.

```
-> user techpubs password writer read-write all-except dshell

-> user techpubs password writer SHA224
-> user techpubs password writer SHA256+3DES

-> user snmpv3user password pass1pass1 priv-password priv1priv1 read-write all
sha+aes

-> user snmpv3user password pass1pass1 prompt-priv-passwd
   Enter privacy password:   *********
   Re-enter privacy password: *********
```

Release History

Release 6.6.1; command was introduced.
Release 6.7.1.R02; **password-prompt**, **all-except**, additional options for **SHA224** and **SHA256** algorithms, **priv-password** parameter added.
Release 6.7.1.R04; **prompt-priv-passwd** parameter added.
Release 6.7.2.R03; admin user password in SHA2.
Release 6.7.2.R04; *viewname* parameter 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
   aaauSnmpPrivPassword
```

password

Configures the current user's password.

password

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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**, **copy running-config working**, or **configuration snapshot** command is not required to save password settings over a reboot.

Examples

```
-> password
enter old password: ********
enter new password: *********
reenter new password: *********
->
```

Release History

Release 6.6.1; 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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> user password-size min 9
```

Release History

Release 6.6.1; 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-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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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-lowercase *number*

Syntax Definitions

number	The minimum number of lowercase characters. The range is 0 to 7.

Defaults

parameter	default
number	0

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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**, **copy running-config working**, or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-window 500
-> user lockout-window 0
```

Release History

Release 6.6.1; 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 6450, 6350

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**, **copy running-config working**, or **configuration snapshot** command to save user settings over a reboot.
- User lockout threshold settings is not applicable for SSH. Unlike Telnet session, SSH have server and client configuration files, the password prompt will work according to its SSH configuration file.

Examples

```
-> user lockout-threshold 3
-> user lockout-threshold 0
```

Release History

Release 6.6.1; 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 6450, 6350

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**, **copy running-config working**, or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-duration 60
-> user lockout-duration 0
```

Release History

Release 6.6.1; 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 *profile* **{lockout | unlock}**

Syntax Definitions

profile	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 6450, 6350

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**, **copy running-config working**, or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user j_smith lockout
-> user j_smith unlock
```

Release History

Release 6.6.1; 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 can only be used with 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 the user's device.
slot/port	The slot and port number of the specific switch. All users learned on this port are logged out.
user_name	The user name of the account to log out.
profile_name	The name of the User Network Profile (UNP). All users classified with this profile are logged out of the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command can only be used by the user with administrative privileges.
- 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 6.6.3; command was introduced.

Related Commands

show aaa-device all-users	Displays the information about the users (both supplicant and non supplicant) logged into the switch.

MIB Objects

```
alaDot1xAdminLogoutParams
   alaDot1xAdminLogoutType
   alaDot1xAdminLogoutMacAddress
   alaDot1xAdminLogoutUserName
   alaDot1xAdminLogoutNetworkProfileName
   alaDot1xAdminLogoutInterfaceId
```

system common-criteria

Enables or disables common criteria mode on the switch.

system common-criteria admin-state {enable | disable}

Syntax Definitions

enable | disable	Enables or disables the common criteria mode.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The configuration is applied only after a reload of the switch.
- When you login to the switch after enabling Common Criteria, you will be prompted to change your password. Passwords length should be of 15 characters or greater.
- Common-Criteria and ASA enhanced-mode (NIS) are mutually exclusive features. If the switch is already running in enhanced mode, the user is not allowed to configure Common-Criteria.

Examples

```
-> system common-criteria enable
WARNING: Common Criteria configuration is applied only after REBOOT
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

show system common-criteria	Displays the configured and running status of common criteria mode on the switch.

MIB Objects

N/A

show system common-criteria

Displays the configured and running status of common criteria mode on the switch.

show system common-criteria

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

After enabling the common criteria on the switch, if the common criteria mode running status is showing as “Disabled”, you need to reboot the switch to for common criteria mode to come into effect.

Examples

```
-> show system common-criteria
Common Criteria mode Configured status: Enabled
Common Criteria mode Running status: Enabled

-> show system common-criteria
Common Criteria mode Configured status: Enabled
Common Criteria mode Running status: Disabled
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

system common-criteria	Enables or disables common criteria mode on the switch.

MIB Objects

N/A

aaa certificate update-ca-certificate

Updates the CA-bundle with the custom CA server certificate provided by CA.

aaa certificate update-ca-certificate *ca_file*

Syntax Definitions

ca_file	The custom CA server certificate (in PEM format) provided by the CA.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The custom CA server certificate should be copied in PEM format to the **/flash/switch/** directory via SFTP.
- This command appends the existing CA bundle (**certs.pem**) and the custom CA server certificate provided as input.
- The update of custom CA server certificates needs to be done before corresponding server configurations are done on the switch. If the update is done post server configuration, then a switch reboot needs to be done for the changes to take effect.

Examples

```
-> aaa certificate update-ca-certificate cert.txt
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

aaa certificate update-crl	Updates the CRL list with the custom CRL provided by CA.

MIB Objects

N/A

aaa certificate update-crl

Updates the CRL list with the custom CRL provided by CA.

aaa certificate update-crl *crl_file*

Syntax Definitions

crl_file	The custom CRL file (in PEM format) provided by the CA.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The custom CRL file should be copied in PEM format to the **/flash/switch/** directory via SFTP.
- This command appends the existing CRL file (**crl.pem**) and the custom CRL provided as input.
- The update of the custom CRL needs to be done before corresponding server configurations are done on the switch. If the update is done post server configuration, then a switch reboot needs to be done for the changes to take effect.

Examples

```
-> aaa certificate update-crl crl.txt
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

aaa certificate update-ca-certificate	Updates the CA-bundle with the custom CA server certificate provided by CA.

MIB Objects

N/A

aaa certificate generate-rsa-key key-file

Generates the RSA 2048 bit key with the file name provided as input.

aaa certificate generate-rsa-key key-file *key_file*

Syntax Definitions

key_file	The name of the key file under which the RSA 2048 bit key is stored.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Generates RSA 2048 bit key in **/flash/switch** directory with the file name as the input key file.

Examples

```
-> aaa certificate generate-rsa-key key-file clientkey.key
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

aaa certificate generate-self-signed	Generates the X.509 self-signed certificate for TLS client authentication.
aaa certificate view	Displays the contents of the X.509 certificate.
aaa certificate delete	Deletes the X.509 certificate.

MIB Objects

N/A

aaa certificate generate-self-signed

Generates the X.509 self-signed certificate for TLS client authentication.

aaa certificate generate-self-signed key-file {*key_file***} [days** *valid_period***} {CN** *common_name***} {ON** *org_name***} {OU** *org_unit***} {L** *locality***} {ST** *state***} {C** *country***}**

Syntax Definitions

key_file	The name of the key file under which the RSA 2048 bit key is stored.
valid_period	Validity period (in days) of the X.509 certificate.
common_name	Common Name used in X.509 certificate.
org_name	The Organization Name used in X.509 certificate.
org_unit	The Organization Unit used in X.509 certificate.
locality	The Locality used in X.509 certificate.
state	The State used in X.509 certificate.
country	The Country used in X.509 certificate.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command generates the file in **/flash/switch** directory.
- All parameters in the CLI are mandatory, there are no optional parameters.
- The client certificate and private key for mutual authentication should to be named as “client-cert.pem” and “client-key.pem” and placed in **/flash/switch** directory.
- The X.509 certificate needs to be done before corresponding server configurations are done on the switch. If the certificate is created post server configuration, then a switch reboot needs to be done for the changes to take effect.

Examples

```
-> aaa certificate generate-self-signed key-file clientkey.key days 3650 cn
client.ale.com on ALE ou ESD l BAN st KAR c IN
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

aaa certificate generate-rsa-key key-file	Generates the RSA 2048 bit key with the file name provided as input.
aaa certificate view	Displays the contents of the X.509 certificate.
aaa certificate delete	Deletes the X.509 certificate.

MIB Objects

N/A

aaa certificate view

Displays the contents of the X.509 certificate.

aaa certificate view *cert_file*

Syntax Definitions

cert_file	The X.509 certificate file (in PEM format) to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> aaa certificate view clientcert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=in, ST=tn, L=shol, O=ale, OU=esd, CN=client.ale.con
        Validity
            Not Before: Sep  2 01:35:47 2016 GMT
            Not After : Dec 31 01:35:47 2016 GMT
        Subject: C=in, ST=tn, L=shol, O=ale, OU=esd, CN=client.ale.con
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f0:e8:d0:8c:57:fe:dd:30:1c:ac:36:2d:1d:ea:
                    0e:69:e0:16:38:72:97:c9:3b:f7:7e:42:c2:f1:7a:
                    08:17:41:e8:e8:36:3c:59:1a:c4:a8:1d:17:e2:85:
                    12:dd:a4:c2:a8:4b:8d:a2:ff:9b:a6:83:dc:21:ad:
                    54:25:e1:cb:73:31:8e:fa:32:b0:89:22:1d:be:3b:
                    31:b2:99:53:f3:0e:dc:18:fe:88:f3:66:ce:66:8a:
                    96:7f:3d:c0:32:37:fa:76:97:c4:fd:e4:7d:08:dd:
                    a9:dd:42:a2:81:8a:4b:79:40:7a:ed:54:d8:d5:4f:
                    81:b5:c3:df:30:fb:e4:48:33:78:4c:15:76:f9:90:
                    c0:70:a7:3a:4d:21:ed:49:c5:f5:af:58:b5:19:43:
                    b9:83:2d:30:b5:b1:d3:dd:9e:25:3f:e2:74:22:0d:
                    78:5b:76:93:d8:be:f7:22:0e:2a:5f:54:78:01:79:
                    15:77:ff:6a:9b:00:6f:6f:ba:11:fc:7a:77:e3:c8:
                    fc:9b:7a:7e:e1:5b:fd:55:c6:5d:7a:a4:2b:7a:71:
                    ae:28:70:de:a5:7d:dc:32:2d:a0:50:e6:52:20:e2:
                    4a:7e:6d:6f:ea:c0:f4:19:64:f7:73:b0:96:19:aa:
```

```
                    63:97:e7:58:fd:6f:0e:f2:96:5b:97:cb:f7:44:b7:
                    a8:bd
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Basic Constraints: critical
                    CA:TRUE
                X509v3 Key Usage: critical
                    Certificate Sign, CRL Sign
                X509v3 Extended Key Usage:
                    TLS Web Client Authentication
        Signature Algorithm: sha1WithRSAEncryption
             b4:b0:66:ce:13:8d:d0:b5:ff:f4:5f:1f:96:07:97:20:f3:a2:
             05:f0:0b:00:e5:f9:36:2f:fd:de:3a:ec:ab:95:73:e7:4f:22:
             c3:06:7a:2b:9f:0f:fc:e4:35:9c:02:14:98:9d:c4:38:c1:0b:
             62:fb:37:d5:3b:f1:e3:15:fd:23:1f:c0:1f:29:dd:ef:c3:35:
             dc:89:78:ce:c4:8d:a5:89:3c:81:de:9b:70:98:38:a4:e4:92:
             8c:d2:f2:b8:4f:b4:19:e2:55:ad:c6:cc:db:61:56:1e:eb:da:
             00:b1:f3:e5:fc:fd:11:b7:ae:6f:aa:ae:3e:5f:b8:cd:22:5a:
             57:01:86:de:44:90:5c:74:7a:bc:07:45:b2:f1:8b:ab:48:e4:
             33:be:da:34:e4:85:76:ea:bc:fd:d5:14:56:31:f4:d8:dc:79:
             56:5e:d1:cf:2f:0f:5d:f9:8f:9b:be:da:8f:65:fb:e4:64:2d:
             60:8f:e4:2d:25:16:8c:9a:27:9a:61:26:7f:64:9e:d9:56:43:
             24:4e:04:ed:e8:67:2d:a9:e2:e6:97:f2:b4:35:d8:0c:62:8c:
             6d:0f:34:e7:f0:4e:8f:bb:3e:cc:de:44:f2:ad:72:09:51:21:
             7f:a1:42:dc:39:bb:c6:b7:81:da:c5:fe:eb:b1:18:ba:f3:a0:
             e2:d0:0f:14
-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIBADANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJpbjEL
MAkGA1UECAwCdG4xDTALBgNVBAcMBHNob2wxDDAKBgNVBAoMA2FsZTEMMAoGA1UE
CwwDZXNkMRcwFQYDVQQDDA5jbGllbnQuYWxlLmNvbjAeFw0xNjA5MDIwMTM1NDda
Fw0xNjEyMzEwMTM1NDdaMF4xCzAJBgNVBAYTAmluMQswCQYDVQQIDAJ0bjENMAsG
A1UEBwwEc2hvbDEMMAoGA1UECgwDYWxlMQwwCgYDVQQLDANlc2QxFzAVBgNVBAMM
DmNsaWVudC5hbGUuY29uMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
8OjQjFf+3TAcrDYtHeoOaeAWOHKXyTv3fkLC8XoIF0Ho6DY8WRrEqB0X4oUS3aTC
qEuNov+bpoPcIa1UJeHLczGO+jKwiSIdvjsxsplT8w7cGP6I82bOZoqWfz3AMjf6
dpfE/eR9CN2p3UKigYpLeUB67VTY1U+BtcPfMPvkSDN4TBV2+ZDAcKc6TSHtScX1
r1i1GUO5gy0wtbHT3Z4lP+J0Ig14W3aT2L73Ig4qX1R4AXkVd/9qmwBvb7oR/Hp3
48j8m3p+4Vv9VcZdeqQrenGuKHDepX3cMi2gUOZSIOJKfm1v6sD0GWT3c7CWGapj
l+dY/W8O8pZbl8v3RLeovQIDAQABozgwNjAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud
DwEB/wQEAwIBBjATBgNVHSUEDDAKBggrBgEFBQcDAjANBgkqhkiG9w0BAQUFAAOC
AQEAtLBmzhON0LX/9F8flgeXIPOiBfALAOX5Ni/93jrsq5Vz508iwwZ6K58P/OQ1
nAIUmJ3EOMELYvs31Tvx4xX9Ix/AHynd78M13Il4zsSNpYk8gd6bcJg4pOSSjNLy
uE+0GeJVrcbM22FWHuvaALHz5fz9Ebeub6quPl+4zSJaVwGG3kSQXHR6vAdFsvGL
q0jkM77aNOSFduq8/dUUVjH02Nx5Vl7Rzy8PXfmPm77aj2X75GQtYI/kLSUWjJon
mmEmf2Se2VZDJE4E7ehnLani5pfytDXYDGKMbQ805/BOj7s+zN5E8q1yCVEhf6FC
3Dm7xreB2sX+67EYuvOg4tAPFA==
-----END CERTIFICATE------
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

aaa certificate generate-self-signed	Generates the X.509 self-signed certificate for TLS client authentication.
aaa certificate delete	Deletes the X.509 certificate.

MIB Objects

N/A

aaa certificate delete

Deletes the X.509 certificate.

aaa certificate delete *cert_file*

Syntax Definitions

cert_file	The X.509 certificate file (in PEM format) to be deleted.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> aaa certificate delete clientcert.pem
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

aaa certificate generate-self-signed	Generates the X.509 self-signed certificate for TLS client authentication.
aaa certificate view	Displays the contents of the X.509 certificate.

MIB Objects

N/A

aaa certificate generate-csr

Generates the CSR (Certificate Signing Request) to be sent to get a CA signed certificate for TLS client authentication.

aaa certificate generate-csr key-file {*key_file***}{CN** *common_name***} {ON** *org_name***} {OU** *org_unit***} {L** *locality***} {ST** *state***} {C** *country***}**

Syntax Definitions

key_file	The name of the key file under which the RSA 2048 bit key is stored.
common_name	Common Name used in X.509 certificate.
org_name	The Organization Name used in X.509 certificate.
org_unit	The Organization Unit used in X.509 certificate.
locality	The Locality used in X.509 certificate.
state	The State used in X.509 certificate.
country	The Country used in X.509 certificate.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Generates *aosCertRequest.pem* file in **/flash/switch** directory.
- All parameters in the CLI are mandatory, there are no optional parameters.
- The CSR needs to be created, sent to CA authority and the corresponding CA certificate (obtained from CA authority) should be uploaded to the **/flash/switch** directory before corresponding server configurations are done on the switch. If the CA certificate is uploaded post server configuration, then a switch reboot needs to be done for the changes to take effect.

Examples

```
-> aaa certificate generate-csr key-file clientkey.key days 3650 cn client.ale.com
on ALE ou ESD L BAN st KAR c IN
```

Release History

Release 6.7.1 R04; command introduced.

Related Commands

show system common-criteria Displays the common criteria status on the switch.

MIB Objects

N/A

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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

aaa admin-logout	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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

aaa admin-logout	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. UNP determines:

- the VLAN ID a device can join,
- whether or not a Host Integrity Check (HIC) is applied to the device,
- whether to assign redirection URL to ClearPass Server for BYOD devices for CoA authorization,
- if any QoS policy rules are used to control access to network resources,
- the maximum ingress and egress bandwidth associated with the UNP,
- maximum default depth associated with the UNP.

aaa user-network-profile name *profile_name* **vlan** *vlan-id* **[hic {enable | disable}] [redirect** *url_name***] [policy-list-name** *list_name***] [maximum-ingress-bandwidth** *num* **[K(kilo) | M(mega)| G (giga)| T (tera)]] [maximum-egress-bandwidth** *num* **[K(kilo) | M(mega)| G (giga)| T (tera)]] [maximum-default-depth** *num* **[K(kilo) | M(mega)| G (giga)| T (tera)]]**

no aaa user-network-profile name *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 a preconfigured 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.
url_name	The redirect URL name of maximum 32 characters associated with a corresponding URL. A maximum of 5 redirect URLs and URL names can be configured.
list_name	The name of an existing QoS policy list to apply to devices classified by the UNP. It is possible to assign up to eight policy lists to each user profile.
num	Maximum ingress bandwidth associated to a UNP. The valid range is 0 - 10485760 (Kbit/sec).
K | M | G | T	The denominator for the ingress bandwidth configured. It can be specified as K (kilo), M (mega), G (giga), and T (tera).
num	Maximum egress bandwidth associated to a UNP. The valid range is 0-1000000 (Kbit/sec).
K | M | G | T	The denominator for the egress bandwidth configured. It can be specified as K (kilo), M (mega), G (giga), and T (tera).
num	Maximum default depth associated to a UNP. The valid range is 0 - 16384 in Kilobytes.
K | M | G | T	The denominator for the default depth configured. It can be specified as s K (kilo), M (mega), G (giga), and T (tera).

Defaults

parameter	default
hic enable | disable	disabled
url_name	none
list_name	none
maximum-ingress-bandwidth **maximum-egress-bandwidth**	No bandwidth limitation is applied.
maximum-default-depth	Optimal default depth value of 1Mbyte is applied.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to remove a UNP from the switch configuration.
- This command is used only with RADIUS as the authentication server.
- Enabling the **hic** parameter triggers the HIC verification process for the devices to which this profile is applied. The switch interacts with the InfoExpress CyberGatekeeper HIC server to determine host compliance.
- Assign a URL name with the **redirect** parameter to specify the redirection URL to ClearPass Server for CoA authorization for BYOD devices. The URL name is associated with a URL link to the redirection server using the **aaa redirect url** command.
- Configure Redirect Server with Clearpass IP using the **aaa redirect-server** command, Redirect URL using **aaa redirect url** and associate Redirect URL to UNP using **aaa user-network-profile** command.
- When HIC is enabled, redirection URL cannot be enabled. HIC must be disabled before applying **redirect** parameter. The **hic** and **redirect** settings are mutually exclusive.
- The egress and ingress bandwidth, and default depth configuration is supported for supplicant, non-supplicant, and captive portal users.
- The egress and ingress bandwidth, and default depth can be configured in kilo (K), mega (M), giga (G), or tera (T) unit or denominator. If no unit is specified while configuring the bandwidth, then the bandwidth value is considered to be in Kbit/sec. In case of default depth, the value is considered to be in Kbytes/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.

Note. The maximum ingress and egress bandwidth allowed is 10485760 (Kbit/sec). To represent the value in tera denomination, convert the value to equivalent of tera. For default depth, to represent the value in mega and tera, convert the required values to equivalent of mega and tera.

- The configured bandwidth is displayed in the show command output with denominator marked as "K", "M", "G" rounded off by maximum two decimal points. For example, the maximum ingress bandwidth of 20000 Kbit/sec, and 2000000 Kbit/sec is displayed as 20.0M and 2.0G.
- When maximum ingress and maximum egress bandwidth is set to 0, no traffic is dropped.
- When maximum default depth is set to '0', the optimal default depth of 1Mbyte is used.
- If QoS policy rule and UNP profile with policy list are both configured, then the lower bandwidth of the two configurations is considered.
- If QoS policy rule and UNP profile without policy list is configured, then the UNP bandwidth is considered.
- If QoS policy rule is of egress type and the UNP profile is configured with or without policy list, then the lower bandwidth of the two configurations is considered.
- When 802.1x is disabled on the port or when interface is administratively brought down, the bandwidth set by UNP on 802.1x port is removed. In both cases, the bandwidth reverts to the bandwidth set by QoS port, if any.
- If multiple users are authenticated on a port, then the latest user authenticated overwrites the previously set bandwidth value. If there is no bandwidth associated to a UNP, no rate limitations are enforced, previously set bandwidth is not changed. Refer to *OmniSwitch AOS Release 6 Network Configuration Guide* for more information.
- Use the **show 802.1x rate-limit** command (see Chapter 50, "802.1x Commands") to view the current rate limit configuration on 802.1x enabled ports.

Examples

```
-> aaa user-network-profile name engineering vlan 10
-> aaa user-network-profile name accounting vlan 20
-> 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
-> aaa user-network-profile name profile1 vlan 50 maximum-ingress-bandwidth 1024
maximum-egress-bandwidth 256 maximum-default-depth 128
-> aaa user-network-profile name unp1 vlan num 172.26.36.26 redirect url url_name
http://clearpass.user.registration.page

-> no aaa user-network-profile name engineering
```

Release History

Release 6.6.1; command was introduced.
Release 6.6.4; **maximum-ingress-bandwidth**, **maximum-egress-bandwidth**, **maximum-default-depth** parameters added.
Release 6.6.5; **redirect** parameter added.

Related Commands

show aaa user-network-profile	Displays the user network profile table.
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.
aaa redirect url	Specifies the different type of URL names that are applied on the redirection UNP.

MIB Objects

```
aaaUserNetProfileTable
   aaaUserNetProfileName
   aaaUserNetProfileVlanID
   aaaUserNetProfileHICflag
   aaaUserNetProfileQosPolicyListName
   aaaUserNetProfileMaxIngressBw
   aaaUserNetProfileMaxEgressBw
   aaaUserNetProfileMaxDefaultDepth
   aaaUserNetworkProfileRedirectUrl
```

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 (for example, 00:00:39:59:f1:0c).
profile_name	The name of an existing UNP.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 with 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.
- 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 6.6.1; 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.
aaa classification-rule lldp med-endpoint	Configures an LLDP 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 radius nas-identifier

Configures the NAS identifier which specifies originating NAS device sending access request frame.

aaa radius nas-identifier { user-string *text_string* **| default }**

Syntax Definitions

text_string	A text string used to define a NAS-identifier for the NAS-Identifier attribute.
default	System name would be sent in access-request packets.

Defaults

By default, the value of NAS-identifier is default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to specify originating NAS device that is sending access-request frames.
- Maximum length of NAS identifier is 31.
- If NAS identifier is configured using user text string, then user-defined NAS identifier will be used.
- If NAS identifier is configured for default value, then system name would be sent in the access-request frames.

Examples

```
-> aaa radius nas-identifier user-string "hello"
-> aaa radius nas-identifier default
```

Release History

Release 6.7.2.R03; command was introduced.

Related Commands

show aaa radius config	Displays the global AAA attribute values.

MIB Objects

```
alaAaaRadNasIdentifier
```

aaa radius nas-ip-address

Configure the NAS-IP address for the outgoing RADIUS packets.

aaa radius nas-ip-address {default | local-ip [*ip_address***] }**

Syntax Definitions

default	Sets the IP address of the NAS that is used by the Radius server to identify the switch.
local-ip	Sets the NAS IP address attribute with the DHCP-Client interface as the device identifier.
ip_address	The IPv4 address for NAS IP address attribute in RADIUS packets.

Defaults

By default, the value of NAS-IP address is default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Configure the IP address to fill the NAS IP address attribute in the RADIUS packets.
  NAS IP address attribute with following priority such as:
  - If IP Managed Interface is configured for RADIUS.
  - If Loopback0 is configured.
  - User configured IP Address in CLI command.
  - IP from IP stack (through which the radius server is reachable).
- Use Local IP to fill NAS IP address attribute with the DHCP client interface.
  NAS IP address attribute with following priority such as:
  - If IP Managed Interface is configured for RADIUS.
  - If Loopback0 is configured.
  - If DHCP Client Interface is configured.
  - IP from IP stack (through which the radius server is reachable).
- Use default option to fill NAS IP address attribute with following priority such as .
  - If IP Managed Interface is configured for RADIUS.
  - If Loopback0 is configured.
  - IP from IP stack (through which the RADIUS server is reachable)

Examples

```
-> aaa radius nas-ip-address default
-> aaa radius nas-ip-address local-ip
-> aaa radius nas-ip-address local-ip 12.12.12.12
```

Release History

Release 6.7.2.R05; command was introduced.

Related Commands

show aaa radius config	Displays the global AAA attribute values.

MIB Objects

```
alaAaaRadClientNasIpAddr
   alaAaaRadNasIpState
   alaAaaRadNasIpField
```

show aaa radius config

Displays the global AAA attribute values.

show aaa radius config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to display the global AAA attribute values.
- By default, the nas-ip-address field will be displayed as default.
- When the IP Address is configured for nas-ip-address attribute then IP address will be displayed.
- When the command **aaa radius nas-ip-address** is configured without IP address then nas-ip-address attribute will be displayed as “dhcp-client Ip”.

Examples

```
-> show aaa radius config
RADIUS client attributes:
  NAS identifier = default
  NAS IP Address = default

-> show aaa radius config
RADIUS client attributes:
  NAS identifier = default
  NAS IP Address = local-ip

-> show aaa radius config
RADIUS client attributes:
  NAS identifier = default
  NAS IP Address = 12.12.12.12
```

Release History

Release 6.7.2.R03; command was introduced.
Release 6.7.2.R05; command modified to display NAS IP address.

Related Commands

aaa radius nas-identifier	Configures the NAS identifier which specifies originating NAS device sending access request frame.
aaa radius nas-ip-address	Configure the NAS-IP address for the outgoing RADIUS packets.

MIB Objects

```
alaAaaRadNasIdentifier
```

aaa classification-rule mac-address-range

Defines a 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 (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).
profile_name	The name of an existing user network profile.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 with 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.
- 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 6.6.1; 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.
aaa classification-rule lldp med-endpoint	Configures an LLDP 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 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 (for example, 10.0.0.0, 171.15.0.0, 196.190.254.0)
subnet_mask	Class A, B, or C subnet mask (for example, 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 6450, 6350

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 with 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.
- 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 6.6.1; 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.
aaa classification-rule lldp med-endpoint	Configures an LLDP UNP mobile rule.
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 classification-rule lldp med-endpoint

Defines a Link Layer Discovery Protocol (LLDP) mobile rule for the specified UNP profile. This rule is used specifically for OmniAccess Stellar Access Point (AP) devices. UNP mobile rules are applied using an Access Guardian Group Mobility device classification policy.

aaa classification-rule lldp med-endpoint access-point user-network-profile name *profile_name*

Syntax Definitions

profile_name	The name of an existing UNP profile.

Defaults

By default, the LLDP classification rule for access points is implicitly created and assigned to the “defaultWLANProfile” when the switch boots up.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The “built-in” LLDP rule and profile facilitates the automatic detection and classification of OmniAccess Stellar APs. When LLDP TLVs from an AP device are detected on an 802.1x port, the device is automatically classified and assigned to the “defaultWLANProfile”.
- Consider the following regarding the built-in LLDP classification rule and “defaultWLANProfile”:
  - The rule and profile cannot be removed from the switch configuration. However, the profile designation for the rule can be changed.
  - The rule does not appear in the configuration snapshot for the switch unless the profile assignment for the rule was changed.
  - Configuring the mapping of a VLAN ID to the “defaultWLANProfile” is required; only the profile itself is implicitly created, not the profile mapping.
  - The mapped VLAN serves as the management VLAN for untagged traffic received from the AP devices that were assigned to the “defaultWLANProfile”.
- 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.
- UNP mobile rules take precedence over VLAN mobile rules.

Examples

```
-> aaa classification-rule lldp med-endpoint access-point user-network-profile name
AP-Group1-Profile
-> aaa classification-rule lldp med-endpoint access-point user-network-profile name
defaultWLANProfile
```

Release History

Release 6.7.2.R02; 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.
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

```
aaaUNPLldpRuleConfig
   aaaUNPLldpRuleProfileName
```

aaa byod white-list

This command is used to configure a white list of IP address to be bypassed by the redirect server which was provided by CPPM server.

[no] aaa byod white-list *ip_address* **[***subnet_mask***]**

Syntax Definitions

ip_address	The IP address of the server to be bypassed.
subnet_mask	A valid IP address mask to identify the IP subnet for the server.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command can be used when users in a restricted role are trying to reach an OCSP server to validate a certificate. Since the users are not authenticated they may continuously be redirected. Adding the OSCP server to a white list will allow the restricted users to reach the OCSP server.
- A Maximum of 8 IP addresses can be configured.

Examples

```
-> aaa byod white-list 192.168.50.50 mask 255.255.255.0
```

Release History

Release 6.6.5; command was introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

show byod status	Displays the status of the BYOD clients at switch or per port level.
show aaa byod white-list ip-address	Displays the status of the BYOD white list IP addresses.

MIB Objects

```
aaaBYODWhiteListTable
   aaaBYODWhiteListIPAddress
   aaaBYODWhiteListIPMask
```

aaa byod white-list no

This command is used to remove a white list of IP address to be bypassed by the redirect server which was provided by CPPM server.

aaa byod white-list no *ip_address*

Syntax Definitions

ip_address	The IP address of the server to be bypassed.
subnet_mask	A valid IP address mask to identify the IP subnet for the server.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- For configuring the BYOD whitelist, use the command **aaa byod white-list**

Examples

```
-> aaa byod white-list 192.168.50.50 mask 255.255.255.0
```

Release History

Release 6.6.5; command was introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

show byod status	Displays the status of the BYOD clients at switch or per port level.
show aaa byod white-list ip-address	Displays the status of the BYOD white list IP addresses.

MIB Objects

```
aaaBYODWhiteListTable
   aaaBYODWhiteListIPAddress
   aaaBYODWhiteListIPMask
```

aaa hic server-name

Configures the identity of the Host Integrity Check (HIC) InfoExpress CyberGatekeeper server. HIC is a 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* {**key** *key* **| prompt-key} [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.
key	The shared key known to the switch and the server, but not sent over the network. This key can be any text or hexadecimal string, but must match the key configured on the server. The key is case sensitive.
prompt-key	This option allows to enter the shared key in a masked format rather than as clear text. When this option is selected, press the Enter key. A prompt appears prompting to enter the shared key. Key needs to be re-entered, and only if both entries match, command is accepted. Key provided in this mode is not displayed on the CLI as text.
primary | backup	Configures the 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 6450, 6350

Usage Guidelines

- Configure the HIC server identity and related parameters before globally enabling the HIC feature for the switch.
- The primary server is initially configured as an active server and the backup server as an inactive server.
- 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 retain the active server upon receiving the keepalive acknowledgment.

- The switch will send a total of four keepalive messages to the active server on every interval of six second. 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 configured HIC Server failure mode.
- 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 key wwwtoe role primary
-> aaa hic server-name hic-srv1 ip-address 2.2.2.2 key wwwtoe udp-port 12049
-> aaa hic no server-name hic-srv1

-> aaa hic server-name hic1 ip-address 1.1.1.1 prompt-key
Enter Key:  *******
Re-enter Key:   *******
```

Release History

Release 6.6.3; command was introduced.
Release 6.7.1 R04; **prompt-key** parameter added.

Related Commands

show aaa priv hexa	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.
aaa classification-rule mac-address	Displays information about AAA servers.
aaa classification-rule mac-address	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 allowed-name

Configures a list of servers that are excluded from the Host Integrity Check (HIC) process. This list identifies the 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* **[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 6450, 6350

Usage Guidelines

- Use the **no** form of the command to remove a server from the HIC exception list.
- Up to four server exception entries are allowed.
- If a host device requires access to the HIC server through a Web-based agent, ensure 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 6.6.3; command was introduced.

Related Commands

aaa classification-rule mac-address	Displays information about AAA servers.
aaa byod white-list	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 6450, 6350

Usage Guidelines

- Configure the HIC server information before enabling the HIC on the switch.
- When HIC is enabled on the switch, reconfiguring the HIC server parameters is not allowed.
- VLAN Stacking feature is not available when HIC is configured on the switch as these two features are mutually exclusive. Only one of them can run on the switch at any given time.

Examples

```
-> aaa hic enable
-> aaa hic disable
```

Release History

Release 6.6.3; command was introduced.

Related Commands

aaa classification-rule mac-address	Displays information about AAA servers.
aaa byod white-list	Configures a HIC server for use with the switch.
aaa classification-rule mac-address	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 6450, 6350

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 6.6.3; command was introduced.

Related Commands

show aaa hic	Displays the global HIC configuration for the switch.
aaa byod white-list	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	Globally enables the HIC feature for the switch.

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 6450, 6350

Usage Guidelines

This command overwrites the existing proxy port number.

Examples

```
-> aaa hic custom-proxy-port 8878
```

Release History

Release 6.6.3; 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
```

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 6450, 6350

Usage Guidelines

- If the primary server is unavailable and in the inactive mode, the switch begins to poll the primary server in the background.
- To avoid overwhelming a primary server that becomes active again, the switch generates a random reconnect value. When the switch receives continuous keepalive responses equal to the random reconnect value it considers the primary server is ready to takeover the active role.
- When the backup server is inactive this interval determines the frequency 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 6.6.3; command was introduced.

Related Commands

show aaa priv hexa	Displays hexadecimal values for command domains/families.

MIB Objects

```
aaaHicConfigInfo
   aaaHicBgPollInterval
```

aaa hic server-failure mode

Configures the failure mode to be applied on the new users when both servers are unavailable.

aaa hic server-failure mode {hold | passthrough}

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 | passthrough	**hold**

Platforms Supported

OmniSwitch 6450, 6350

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 **passthrough** mode, new users will be moved to HIC PASSTHROUGH mode and treated same as HIC SUCCESS.

Examples

```
-> aaa hic server-failure mode passthrough
```

Release History

Release 6.6.3; command was introduced.

Related Commands

show aaa priv hexa	Displays hexadecimal values for command domains/families.

MIB Objects

```
aaaHicConfigInfoTable
   aaaHicSrvFailMode
```

aaa hic server-failure policy user-network-profile change

Configures the network profiles the users are 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 6450, 6350

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 are available, the user is moved back to the original *unp1* and the HIC-check will be restarted.
- A maximum of eight 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 6.6.3; command was introduced.

Related Commands

show aaa priv hexa	Displays hexadecimal values for command domains/families.

MIB Objects

```
aaaHicSvrDownUnpMapTable
   aaaHicSvrDownUnpMapEntry
   aaaHicSvrDownUnpName
   aaaHicSvrDownMappedUnpName
   aaaHicSvrDownUnpRowStatus
```

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 6450, 6350

Usage Guidelines

- If you do not include a server name in the syntax, information for all servers configured in the switch is displayed.
- 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.
- Use this command to view the NAS port, NAS port ID, NAS port type attributes configured for a RADIUS server, and the reachability status of different RADIUS servers configured on the switch.
- Use this command to view the Unique Acct Session ID attribute configured for a RADIUS server.
- The Primary and Backup server information is displayed only if the RADIUS health-check is enabled on the OmniSwitch.
- Use this command to view the RADIUS server statistics such as the server uptime, downtime and number of times server status has changed from down-up and up-down.

Examples

```
-> show aaa server
Server name = ldap2
   Server type= LDAP,
   Host name 1= ors40535,
   Retry number= 3,
   Timeout (in sec)= 2,
   Port= 389,
   Domain name= manager,
   Search base= c=us,
Server name = rad1
   Server type= RADIUS,
   IP Address 1= 10.10.2.1,
   IP Address 2= 10.10.3.5,
   Retry number= 3,
```

```
   Timeout (in sec)= 2,
   Authentication port= 1645,
   Accounting port= 1646,
    Nas port               = default,
   Nas port id             = disable,
   Nas port type           = ethernet,
  Mac Addr Format Status  = disable,
  Mac Address Format      = uppercase,
  Unique Acct Session Id  = disable,
  Health Check Status     = ENABLED,
  Server oper status      = DOWN,
  Primary oper status     = DOWN,
  Backup oper status      = DOWN,
  Polling interval        = 20,
  User name               = alc,
  Failover Status         = ENABLED
Primary server
   Server uptime         = -,
   Server downtime        = MAR 23 2000 01:46:45,
   Nb server up-down     = 0,
   Nb server down-up     = 0,

Backup server
   Server uptime         = MAR 23 2000 01:47:00,
   Server downtime       = -,
   Nb server up-down     = 0,
   Nb server down-up     = 0,


-> aaa tacacs+-server “tacacs” host 172.18.16.99 key alcatel
-> aaa tacacs server-wait-time 4
-> show aaa server tacacs
aaa tacacs server-wait-time 4
Server name = tacacs
   Server type          = TACACS+,
   IP Address 1         = 10.10.5.1,
   Port                 = 49,
   Timeout (in sec)     = 2,
   Encryption enabled   = yes
```

When RADIUS server is configured with NAS port configurations and unique session ID enabled:

```
-> show aaa server
Server name         = Server1
  Server type             = RADIUS,
  IP Address 1            = 172.21.160.26,
  Retry number            = 3,
  Time out (sec)          = 2,
  Authentication port     = 1812,
  Accounting port         = 1813,
  Nas Port               = ifindex,
  Nas Port Id             = disable,
  Nas Port Type           = async
  Mac Addr Format Status  = disable,
  Mac Address Format      = uppercase,
  Unique Acct Session Id  = disable,
  Health Check Status     = ENABLED,
  Server oper status      = DOWN,
```

```
  Primary oper status     = DOWN,
  Polling interval        = 40,
  User name               = adminlab,
  Failover Status         = DISABLED
Primary server
   Server uptime           = -,
   Server downtime         = MAR 23 2000 01:46:45,
   Nb server up-down      = 0,
   Nb server down-up      = 0,

Backup server
   Server uptime         = MAR 23 2000 01:47:00,
   Server downtime        = -,
   Nb server up-down      = 0,
   Nb server down-up      = 0,
```

When RADIUS server is configured with default unique session ID value:

```
-> show aaa server
Server name = Server1
Server type         = RADIUS,
IP Address 1        = 172.21.160.29,
Retry number        = 3,
Time out (sec)      = 2,
Authentication port = 1812,
Accounting port     = 1813,
Nas port            = default,
Nas port id         = disable,
Nas port type       = ethernet,
Unique Acct Session Id = disable,
Health Check Status     = DISABLED,
Server oper status      = UNKNOWN,
Primary oper status     = UNKNOWN,
Polling interval        = 60,
User name               = admin,
Failover Status         = DISABLED
Primary server
   Server uptime           = -,
   Server downtime         = MAR 23 2000 01:46:45,
   Nb server up-down      = 0,
   Nb server down-up      = 0,

Backup server
   Server uptime         = MAR 23 2000 01:47:00,
   Server downtime        = -,
   Nb server up-down      = 0,
   Nb server down-up      = 0,
```

When RADIUS server is configured with Case Sensitive MAC address Authentication:

```
-> aaa tacacs command-authorization enable
-> show aaa server
aaa tacacs command-authorization enable
aaa tacacs server-wait-time 4
Server name = Server1
   Server type          = RADIUS,
   IP Address 1         = 172.21.160.29,
   Retry number         = 3,
   Time out (sec)       = 2,
```

```
    Authentication port  = 1812,
    Accounting port      = 1813,
    Nas port             = default,
    Nas port id          = disable,
    Nas port type        = ethernet,
    MAC Address Format Status  = disable,
    MAC Address Format         = uppercase,
    Unique Acct Session Id     = disable,
    Health Check Status     = DISABLED,
     Server oper status      = UNKNOWN,
     Primary oper status     = UNKNOWN,
     Polling interval        = 35,
     User name               = admin1,
     Failover Status         = DISABLED
Primary server
    Server uptime           = -,
    Server downtime         = MAR 23 2000 01:46:45,
    Nb server up-down      = 0,
    Nb server down-up      = 0,

Backup server
    Server uptime         = MAR 23 2000 01:47:00,
    Server downtime        = -,
    Nb server up-down      = 0,
    Nb server down-up      = 0,

Server name = tacacs
    Server type         = Tacacs+,
    IP Address 1        = 172.18.16.99,
    Port                = 49,
    Time out (sec)      = 2,
Encryption enabled      = yes
-> 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 radius-health-check**, and **aaa ldap-server** commands. Parameters for the ACE server are automatically set by the switch.

output definitions

aaa tacacs command-authorization	The status of command based authorization in TACACS+ server.
aaa tacacs server-wait-time	The wait time of TACACS+ server during command authorization process
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.
NAS Port	NAS port configured for the NAS server.
NAS Port Id	NAS port ID configured for the NAS server.
NAS Port Type	NAS port type configured for the NAS server.
MAC Address Format Status	The MAC address format status (**enable** or **disable**) for Case Sensitive MAC address authentication.
MAC Address Format	The MAC-address-format setting (**uppercase** or **lowercase**). for Case Sensitive MAC address authentication.
Unique Acct Session Id	The status of the unique session ID: Enable or Disable
Server oper status	The status of the RADIUS server: UP, DOWN or UNKNOWN.
Primary oper status	The status of the primary radius server. UP, DOWN or UNKNOWN.
Backup oper status	The status of the backup radius server. UP, DOWN or UNKNOWN.
Polling interval	The interval in which the radius server is polled.
User name	The user name set for the radius server.
Failover status	The failover status set for the radius server.

output definitions

Primary server	Displays the primary RADIUS server uptime and downtime and the number of times status has changed from up-down and down-up.
Backup server	Displays the backup RADIUS server uptime and downtime and the number of times status has changed from up-down and down-up.

Release History

Release 6.6.1; command was introduced.
Release 6.6.4; NAS Port, NAS Port Id, NAS Port Type, MAC Address Format Status, MAC Address Format, Unique Acct Session Id output fields added.
Release 6.7.1.R02; Server oper Status output field added.
Release 6.7.1.R03; Health Check Status, Primary oper status, Backup oper status, Polling interval, User name and Failover status output field added for radius server type.
Release 6.7.2.R03; primary server and back up server statistics output fields added for RADIUS server.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access.
aaa ldap-server	Configures or modifies an LDAP server for Authenticated Switch Access.
aaa radius-health-check	Configures or modifies a TACACS+ server for Authenticated Switch Access.
aaa radius-health-check	Configures the radius health check feature for a specific radius server.

MIB Objects

```
aaaServerTable
   aaasName
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasHostName2
   aaasIpAddress2
   aaasRetries
   aaasTimout
   aaasRadKey
   aaasRadAuthPort
   aaasRadAcctPort
   aaasLdapPort
   aaasLdapDn
   aaasLdapPasswd
   aaasLdapSearchBase
   aaasLdapServType
   aaasLdapEnableSsl
   aaasAceClear
   aaasRowStatus
   aaasTacacsKey
   aaasTacacsPort
   aaasHttpPort
   aaasHttpDirectory
   aaasHttpProxyHostName
```

```
aaasHttpProxyIpAddress
aaasHttpProxyPort
aaasRadMacAddrCaseStatus
aaasRadMacAddrFormat
aaasRadUniqueAcctSessionId
aaaRadServerPrimaryStatus
aaaRadServerBackupStatus
aaaRadPrimSerNbUpToDown
aaaRadPrimSerNbDownToUp
aaaRadPrimServUpTime
aaaRadPrimServDownTime
aaaRadBkupSerNbUpToDown
aaaRadBkupSerNbDownToUp
aaaRadBkupServUpTime
aaaRadBkupServDownTime
```

show aaa radius-health-check config

Displays the radius health check configuration information of radius servers.

show aaa radius-health-check config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

Use the **show aaa radius-health-check config** command to display radius health check configuration information such as polling interval, health check status, username and failover status.

Examples

```
-> show aaa radius-health-check config
Server Name   Polling Interval   Healthcheck status   User Name    Failover
------------+-----------------+--------------------+-----------+-----------------
rad           80                ENABLED               admin      DISABLED
rad1          700               ENABLED              admin1     DISABLED
rad2          60                ENABLED              admin3     DISABLED
```

output definitions

Server Name	Displays the radius server name.
Polling Interval	Displays the configured polling interval for that radius server.
Healthcheck status	Displays the operational status of the radius health check feature for that server.
User Name	Displays the configured user name for radius server polling.
Failover	Displays the operational status of the failover.

Release History

Release 6.7.1 R03; command was introduced.

Related Commands

aaa radius-health-check	Configures the radius health check feature for a specific radius server.

MIB Objects

```
aaasName
   aaasRadPollInterval
   aaasRadHealthstatus
   aaasRadUser
   aaasRadFailoverStatus
```

show radius-server statistics

Displays the authorization, authentication, accounting, and BYOD statistics for the configured radius servers.

show radius-server [*server name***] statistics**

Syntax Definitions

server_name	Provide the server name to view the statistics for a specific server. If the server name is not specified then the statistics for all the configured radius servers will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

To view the statistics for a specific server, provide the server name.

Examples

```
-> show radius-server statistics
Server name = rad1
Authorization stats:
    Nb Access-Req      : 0
    Nb Access-Res      : 0
    Nb Acc-Req Time    : 0
    Last RTT           : 0
    Last week min RTT  : 0
    Last week max RTT  : 0
    Last week avg RTT  : 0
Authentication stats:
    Nb Access-Req      : 0
    Nb Access-Res      : 0
    Nb Access-Chal     : 0
    Nb Access-Accept   : 0
    Nb Access-Reject   : 0
    Nb Acc-Req Time    : 0
    Last RTT           : 0
    Last week min RTT  : 0
    Last week max RTT  : 0
    Last week avg RTT  : 0
Accounting stats:
    Nb Account-Req     : 0
    Nb Account-Res     : 0
    Nb Accnt-Req Time  : 0
    Last RTT           : 0
    Last week min RTT  : 0
```

```
    Last week max RTT  : 0
    Last week avg RTT  : 0
BYOD stats:
    Nb COA-Req         : 0
    Nb COA_ACK         : 0
    Nb COA_NACK        : 0
    Nb DM-Req          : 0
    Nb DM_ACK          : 0
    Nb DM_NACK         : 0
Nb Rx Dropped          : 0
Last clear timestamp   : -
```

output definitions

Authorization	The statistics information displayed for authorization.
Total No of Access-Request	Displays the total number of authorization access-request sent to the server.
Total No of Access-Response	Displays the total number of authorization access-response received from the server.
Total No of Access-Request timedout	Displays the total number of authorization access-request which timedout.
Last RTT of Access-Request/ Response	Displays the last RTT of authorization access-request or response.
Min RTT of Access-Request/ Response	Displays the minimum RTT of authorization access-request or response for last seven days.
Avg RTT of Access-Request/ Response	Displays the average RTT of authorization access-request or response for last seven days.
Max RTT of Access-Request/ Response	Displays the max RTT of authorization access-request or response for last seven days.
Authentication	The statistics information displayed for authentication.
Total No of Access-Request	Displays the total number of authentication access-request sent to the server.
Total No of Access-Response	Displays the total number of authentication access-response received from the server.
Total No of Access-Challenge	Displays the total number of authentication access-challenge received from the server.
Total No of Access-Accept	Displays the total number of authentication access-accept received from the server.
Total No of Access-Reject	Displays the total number of authentication access-reject received from the server.
Total No of Access-Request timedout	Displays the total number of authentication access-request which timedout.
Last RTT of Access-Request/ Response	Displays the last RTT of authentication access-request or response.
Min RTT of Access-Request/ Response	Displays the minimum RTT of authentication access-request or response for last seven days.

output definitions

Avg RTT of Access-Request/ Response	Displays the average RTT of authentication access-request or response for last seven days.
Max RTT of Access-Request/ Response	Displays the maximum RTT of authentication access-request or response for last seven days.
Accounting	The statistics information displayed for accounting.
Total No of Accounting - Request	Displays the total number of accounting access-request sent to the server.
Total No of Accounting - Response	Displays the total number of accounting access-response received from the server.
Total No of Accounting - Request timedout	Displays the total number of accounting access-request which timedout.
Last RTT of Accounting - Request/Response	Displays the last RTT of accounting access-request or response.
Min RTT of Accounting - Request/Response	Displays the minimum RTT of accounting access-request or response for last seven days.
Avg RTT of Accounting - Request/Response	Displays the average RTT of accounting access-request or response for last seven days.
Max RTT of Accounting - Request/Response	Displays the maximum RTT of accounting access-request or response for last seven days.
BYOD	Displays the BYOD statistics.
Total COA request	Displays the total number of COA Request received from the server.
Total COA ACK sent	Displays the total number of COA-ACK sent to the server.
Total COA NACK sent	Displays the total number of COA-NACK sent to the server.
Total Disconnect request	Displays the total number of COA-DISCONNECT request received from the server.
Total Disconnect ACK sent	Displays the total number of COA-DISC acknowledgement sent to the server.
Total Disconnect NACK sent	Displays the total number of COA-DISC NACK sent to the server.

Release History

Release 6.7.2.R03; command was introduced.

Related Commands

aaa radius-health-check	Configures the radius health check feature for a specific radius server.

MIB Objects

```
alaRadAuthorTable
   alaRadAuthorServRef
   alaRadAuthorServNbAccReq
   alaRadAuthorServNbAccRes
   alaRadAuthorServNbAccReqTimed
   alaRadAuthorLastRTT
```

```
   alaRadAuthorMinRTT
   alaRadAuthorAvgRTT
   alaRadAuthorMaxRTT
alaRadAuthTable
   alaRadAuthServNbAccReq
   alaRadAuthServNbAccRes
   alaRadAuthServNbAccCha
   alaRadAuthServNbAccAcpt
   alaRadAuthServNbAccRej
   alaRadAuthServNbAccReqTimed
   alaRadAuthLastRTT
   alaRadAuthMinRTT
   alaRadAuthAvgRTT
   alaRadAuthMaxRTT
alaRadAccTable
   alaRadAccServNbAccReq
   alaRadAccServNbAccRes
   alaRadAccServNbAccReqTimed
   alaRadAccLastRTT
   alaRadAccMinRTT
   alaRadAccAvgRTT
   alaRadAccMaxRTT
alaRadByodTable
   alaRadByodservNbCoaReq
   alaRadByodServNbCoaAck
   alaRadByodServNbCoaNack
   alaRadByodServNbCoaDiscReq
   alaRadByodServNbCoaDiscAck
   alaRadByodServNbCoaDiscNack
```

clear radius-server statistics

Clears the server statistics for the configured radius servers.

clear radius-server [*server_name***] statistics**

Syntax Definitions

server_name	Provide the server name for which the statistics need to be cleared. If the server name is not specified then the statistics for all the configured radius servers will be cleared.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

To clear the statistics for a specific server, provide the server name.

Examples

```
-> clear radius-server statistics
-> clear radius-server rad1 statistics
```

Release History

Release 6.7.2.R03; command was introduced.

Related Commands

aaa radius-health-check	Configures the radius health check feature for a specific radius server.

MIB Objects

N/A

show aaa authentication

Displays information about the current authenticated switch session.

show aaa authentication

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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
   aaatsName5
```

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 6450, 6350

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-vlan-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 6.6.1; command was introduced.

Related Commands

aaa authentication 802.1x	Enables/disables the switch for 802.1X authentication.

MIB Objects

```
AaaAuth8021XTable
   aaatxName1
   aaatxName2
   aaatxName3
   aaatxName4
   aaatxName5
   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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

aaa authentication mac	Enables/disables the switch for MAC-\based authentication.

MIB Objects

```
AaaAuthMACTable
   aaaMacSrvrName1
   aaaMacSrvrName2
   aaaMacSrvrName3
   aaaMacSrvrName4
   aaaMacSrvrName5
```

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 6450, 6350

Usage Guidelines

Accounting servers are configured through the **aaa radius-server**, **aaa radius-health-check**, 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 6.6.1; command was introduced.

Related Commands

aaa accounting 802.1x	Enables/disables accounting for 802.1X authentication sessions.

MIB Objects

```
AaaAcct8021XTable
   aaacxName1
   aaacxName2
   aaacxName3
   aaacxName4
   aaacxName5
```

show aaa accounting mac

Displays information about accounting servers for 802.1X non-supplicant (MAC-based) sessions.

show aaa authentication mac [statistics]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Accounting servers are configured through the **aaa radius-server**, **aaa radius-health-check**, 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.
NSA-users Logged in	Displays the number of non-supplicant users logged in successfully.
NSA-users Logged out	Displays the number of non-supplicant users logged out successfully.
NSA-users Failed info	Displays the number of non-supplicant users whose authentication failed.
NSA-users IntermUpdate	Displays the number of interim updates sent when client obtains IP from DHCP server.

Release History

Release 6.6.3; command was introduced.

Related Commands

aaa accounting mac	Enables/disables accounting for 802.1X non-supplicant (MAC-based) authentication sessions.

MIB Objects

N/A

show aaa accounting

Displays information about accounting servers configured for 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 6450, 6350

Usage Guidelines

Use the **show aaa accounting** command to display 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	*Authenticated VLANs are not supported.*
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 6.6.1; command was introduced.

Related Commands

aaa accounting mac	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
   aaacsName5
```

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 6450, 6350

Usage Guidelines

Use this command to display information about read/write access and partitioned management access (domains and families) or end-user profiles associated with users.

Examples

```
-> show user
User name = admin,
  Password expiration     = None,
  Password allow to be modified date     = None,
  Account lockout     = None,
  Password bad attempts     = 1,
  Read Only for domains   = None,
  Read/Write for domains  = All ,
  Snmp allowed     = NO,
  Console-Only    = Disabled
User name = public,
  Password expiration     = None,
  Password allow to be modified date     = None,
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = All ,
  Snmp allowed     = YES,
  Snmp authentication     = NONE,
  Snmp encryption     = NONE,
  Console-Only    = Disabled
User name = alcatel,
  Password expiration     = None,
  Password allow to be modified date     = None,
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = All ,
  Snmp allowed     = YES,
```

```
  Snmp authentication     = NONE,
  Snmp encryption     = NONE,
  Console-Only    = Disabled
User name = default (*),
  Password expiration     = None,
  Password allow to be modified date     = None,
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = None,
  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.

User name = user_auth1,
  Password expiration     = None,
  Password allow to be modified date     = None,
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = None,
  Snmp allowed     = YES,
  Snmp authentication     = MD5,
  Snmp encryption     = DES,
  Console-Only    = Disabled

-> show user j_smith
User name = user_auth1,
  Password expiration     = None,
  Password allow to be modified date     = None,
  Account lockout     = None,
  Password bad attempts     = 0,
  Read Only for domains   = None,
  Read/Write for domains  = None,
  Snmp allowed     = YES,
  Snmp authentication     = MD5,
  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 is 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 **aaa admin-logout** 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.

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 ip-routing ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-security	session aaa

Release History

Release 6.6.1; command was introduced.

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
```

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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; 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
```

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

user	Configures or modifies user entries in the local user database.

MIB Objects

N/A

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

aaa admin-logout	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.

MIB Objects

N/A

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 6450, 6350

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 6.6.1; command was introduced.

Related Commands

aaa admin-logout	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 6450, 6350

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 depth associated to UNP.

Release History

Release 6.6.3; command was introduced.
Release 6.6.4; 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 | lldp-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.
lldp-rule	Displays Link Layer Discovery Protocol (LLDP) rules.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Specifying a rule type parameter (**mac-rule, mac-range-rule**, **ip-net-rule**, or **lldp-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.

```
-> show aaa classification-rule lldp-rule

MED Endpoint Profile Name
-----------+--------------------------------
Acess-Point  defaultWLANProfile
```

output definitions

MED Endpoint	The LLDP MED Endpoint device to which the UNP is applied. The built-in rule and profile to classify an OmniAccess Stellar AP is displayed.
User Network Profile Name	The name of the UNP applied to the host device.

Release History

Release 6.6.3; command was introduced.
Release 6.7.2.R02; **lldp-rule** parameter added.

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.
aaa classification-rule lldp med-endpoint	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

aaaUNPLldpRuleConfig
   aaaUNPLldpRuleProfileName
```

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 6450, 6350

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 6.6.3; command was introduced.

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 6450, 6350

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 6.6.3; 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 6450, 6350

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 byod white-list** command.
HIC Server IP Address	The IP address of the HIC server. Configured through the **aaa byod white-list** command.
HIC server UDP Port	The UDP port number. Configured through the **aaa byod white-list** command.
HIC Server Role	The role of this server; primary or backup. Configured through the **aaa byod white-list** command.
HIC Server Connection	The server connection status; active or inactive.
HIC Server Status:	The server status; up or down.

Release History

Release 6.6.3; 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-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 allowed

Displays the HIC server exception list. The servers included in this list are exempted 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 6450, 6350

Usage Guidelines

- Use this command to get the list of servers allowed access to the switch and host device as part of the HIC process.
- The HIC server exception list may contain up to four 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 classification-rule mac-address** command.
IP Address	The IP address of the allowed server. Configured through the **aaa classification-rule mac-address** command.
IP Mask	The IP subnet mask for the allowed server. Configured through the **aaa classification-rule mac-address** command.

Release History

Release 6.6.3; 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 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 6450, 6350

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 6.6.3; command was introduced.

Related Commands

aaa byod white-list	Configures the HIC server.

MIB Objects

```
aaaHicSvrDownUnpMapTable
   aaaHicSvrDownUnpMapEntry
   aaaHicSvrDownUnpName
   aaaHicSvrDownMappedUnpName
   aaaHicSvrDownUnpRowStatus
aaaHicConfigInfoTable
   aaaHicSrvFailMode
```

show aaa-device all-users

Displays the information about the users (both supplicant and non supplicant) logged into the switch.

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 6450, 6350

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 Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/1  00:11:50:a6:12:00 User101      100  Brdg 10.133.0.100 1X   Pass   Marketing    plist1
1/1  00:11:50:a6:12:01 User101      100  Brdg 10.133.0.101 1X   Pass   Marketing    plist1
1/1  00:11:50:a6:12:02 User101      100  Brdg 10.133.0.102 1X   Pass   Marketing    plist1
1/1  00:11:50:a6:12:03 User101      100  Brdg 10.133.0.103 1X   Pass   Marketing    plist1
1/2  00:00:39:47:4f:0c pc2006       1000 Brdg -            1X   Pass   Marketing    plist1
1/2  00:b0:d0:77:fa:72 000008854    1000 Brdg -            MAC  Pass   Marketing    plist1
2/39 50:65:f3:1f:15:08 5065F31F1508 1000 Blk  -            MAC  Fail   N/A          N/A
3/2  fc:3f:db:07:9d:bf FC3FDB079DBF 100  Brdg -            MAC  Pass   unp          N/A
3/12 00:00:00:00:00:09 000000000009 100  Brdg -            MAC  Pass   unp          plist2
5/9 00:90:27:17:91:a8  pc2006       1000 Brdg -            1X   Pass   Engineering  plist3
5/9 00:00:39:93:46:0c  000008856    1    Blk  -            MAC  Fail   N/A          N/A

-> show aaa-device all-users unp Marketing

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/1  00:11:50:a6:12:00 User101      100  Brdg 10.133.0.100 1X   Pass   Marketing    plist1
1/1  00:11:50:a6:12:01 User101      100  Brdg 10.133.0.101 1X   Pass   Marketing    plist1
1/1  00:11:50:a6:12:02 User101      100  Brdg 10.133.0.102 1X   Pass   Marketing    plist1
1/1  00:11:50:a6:12:03 User101      100  Brdg 10.133.0.103 1X   Pass   Marketing    plist1
1/2  00:00:39:47:4f:0c pc2006       1000 Brdg -            1X   Pass   Marketing    plist1
1/2  00:b0:d0:77:fa:72 000008854    1000 Brdg -            MAC  Pass   Marketing    plist1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/2  00:00:39:47:4f:0c pc2006       1000 Brdg -            1X   Pass   Marketing    plist1
1/2  00:b0:d0:77:fa:72 000008854    1000 Brdg -            MAC  Pass   Marketing    plist1

-> show aaa-device all-users unp Marketing port 1/2

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/2  00:00:39:47:4f:0c pc2006       1000 Brdg -            1X   Pass   Marketing    plist1
1/2  00:b0:d0:77:fa:72 000008854    1000 Brdg -            MAC  Pass   Marketing    plist1

-> show aaa-device all-users port 5/9

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
5/9 00:90:27:17:91:a8  pc2006       1000 Brdg  -           1X   Pass   Engineering  plist3
5/9 00:00:39:93:46:0c  000008856    1    Blk   -           MAC  Fail   N/A          N/A

-> show aaa-device mac-address 00:00:00:00:88:54

Detail status for device:
  MAC Address                     = 00:00:00:00:88:54
  IP Address                      = None.
  Port                            = 1/1
  Authentication Type             = MAC Authentication
  Authentication Result           = Successful
  Classification Policy           = VLAN ID
  VLAN Learned on                 = 10  (SUN FEB 11 2001  00:26:52 (UTC))
```

```
MAC Address Mode Learnt on System  = Bridging
UserName                          = 000000008854
HIC                                = no
```

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	Displays the user-name entered through MAC authentication, if the user is a MAC user.
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.
Policy List Name	The name of the QoS policy list applied to the user device. If a policy list name is returned from the server, that name is displayed; otherwise, the name of the policy list associated with the local profile is displayed. If **N/A** appears in this field, there is no policy list associated with this device.

Release History

Release 6.6.3; command was introduced.
Release 6.7.2.R02; **User Name** and **Policy List Name** fields added.

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
   alaDot1xDeviceStatusMaclearnedState
   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 6450, 6350

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 Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/1 00:11:50:a6:12:00  User101      100  Brdg 10.133.0.100 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:01  User101      100  Brdg 10.133.0.101 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:02  User101      100  Brdg 10.133.0.102 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:03  User101      100  Brdg 10.133.0.103 1X   Pass   Marketing    plist1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/2 00:00:39:47:4f:0c  pc2006       1000 Brdg -            1X   Pass   Marketing    plist1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
5/9 00:90:27:17:91:a8  pc2006       1000 Brdg -            1X   Pass   Engineering  plist2
5/9 00:00:39:93:46:10  --           1    Blk  -            1X   Fail   N/A          N/A

-> show aaa-device supplicant-users port 5/9

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
5/9 00:90:27:17:91:a8  pc2006       1000 Brdg -            1X   Pass   Engineering  plist2
5/9 00:00:39:93:46:10  --           1    Blk  -            1X   Fail   N/A          N/A

-> show aaa-device supplicant-users authentication-status fail

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
5/9 00:00:39:93:46:10  --           1    Blk  -            1X   Fail   N/A          N/A
```

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.
Policy List Name	The name of the QoS policy list applied to the user device. If a policy list name is returned from the server, that name is displayed; otherwise, the name of the policy list associated with the local profile is displayed. If **N/A** appears in this field, there is no policy list associated with this device.

Release History

Release 6.6.3; command was introduced.
Releasse 6.7.2.R02; **Policy List Name** field added.

Related Commands

show aaa-device all-users	Displays the information about the users (both supplicant and non supplicant) logged into 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
   alaDot1xDeviceStatusMaclearnedState
   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 6450, 6350

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 Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/13 00:00:00:00:2c:83 000000002c83 10   Brdg -            MAC  Pass   Marketing    plist1

-> show aaa-device non-supplicant-users unp unp1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
3/1  00:00:00:00:00:01 000000000001 10   Brdg -            MAC  Pass   unp1         plist2

-> show aaa-device non-supplicant-users unp unp1 port 3/1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
3/1  00:00:00:00:00:01 000000000001 10   Brdg -            MAC  Pass   unp1         plist2

-> show aaa-device non-supplicant-users unp no_internet

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/1 00:1a:50:a6:12:50  --           100  Blk  10.133.2.128 None N/A    no_internet  N/A
1/1 00:1a:50:a6:12:51  --           100  Blk  10.133.2.129 None N/A    no-internet  N/A
1/1 00:1a:50:a6:12:52  --           100  Blk  10.133.2.130 None N/A    no_internet  N/A
1/1 00:1a:50:a6:12:53  --           100  Blk  10.133.2.131 None N/A    no_internet  N/A

-> show aaa-device non-supplicant-users authentication-status success

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/2 00:b0:d0:77:fa:72  --           1000 Brdg -            MAC  Pass   Marketing    plist1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
5/9 00:90:27:17:91:20  pc2006       1000 Brdg  -           MAC  Pass   Engr         plist3
```

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	Displays the user-name entered through MAC authentication, if the user is a MAC user.
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**).

output definitions

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.
Policy List Name	The name of the QoS policy list applied to the user device. If a policy list name is returned from the server, that name is displayed; otherwise, the name of the policy list associated with the local profile is displayed. If **N/A** appears in this field, there is no policy list associated with this device.

Release History

Release 6.6.3; command was introduced.
Release 6.7.2.R02; **User Name** and **Policy List Name** fields added.

Related Commands

show aaa-device all-users	Displays the information about the users (both supplicant and non supplicant) logged into 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
   alaDot1xDeviceStatusMaclearnedState
   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 6450

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 Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/1 00:11:50:a6:12:00  User101      100  Brdg 10.133.0.100 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:01  User101      100  Brdg 10.133.0.101 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:02  User101      100  Brdg 10.133.0.102 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:03  User101      100  Brdg 10.133.0.103 1X   Pass   Marketing    plist1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/2 00:00:39:47:4f:0c  pc2006       1000 Brdg -            1X   Pass   Marketing    plist1
1/2 00:b0:d0:77:fa:72  --           1000 Brdg -            MAC  Pass   Marketing    plist1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
5/9 00:90:27:17:91:a8  pc2007       1000 Brdg -            1X   Pass   Engr         plist2
5/9 00:00:39:93:46:0c  --           1    Blk  -            MAC  Fail   N/A          plist2

-> show aaa-device captive-portal-users unp Marketing

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/1 00:11:50:a6:12:00  User101      100  Brdg 10.133.0.100 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:01  User101      100  Brdg 10.133.0.101 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:02  User101      100  Brdg 10.133.0.102 1X   Pass   Marketing    plist1
1/1 00:11:50:a6:12:03  User101      100  Brdg 10.133.0.103 1X   Pass   Marketing    plist1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/2 00:00:39:47:4f:0c  pc2006       1000 Brdg -            1X   Pass   Marketing    plist1
1/2 00:b0:d0:77:fa:72  --           1000 Brdg -            MAC  Pass   Marketing    plist1

-> show aaa-device captive-portal-users policy vlan

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
1/2 00:00:39:47:4f:0c  pc2006       1000 Brdg -            1X   Pass   Marketing    plist1
1/2 00:b0:d0:77:fa:72  --           1000 Brdg -            MAC  Pass   Marketing    plist1

Slot MAC               User              Addr IP      Authentication User Network Policy List
Port Address           Name         VLAN Mode Address      Type Result Profile Name Name
----+-----------------+------------+----+----+------------+----+------+------------+---------
5/9 00:90:27:17:91:a8  pc2007       1000 Brdg -            1X   Pass   Engr         plist2
5/9 00:00:39:93:46:0c  --           1    Blk  -            MAC  Fail   N/A          plist2
```

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.

output definitions

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.
Policy List Name	The name of the QoS policy list applied to the user device. If a policy list name is returned from the server, that name is displayed; otherwise, the name of the policy list associated with the local profile is displayed. If **N/A** appears in this field, there is no policy list associated with this device.

Release History

Release 6.6.3; command was introduced.
Release 6.7.2.R02; **Policy List Name** field added.

Related Commands

show aaa-device all-users	Displays the information about the users (both supplicant and non supplicant) logged into 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
   alaDot1xDeviceStatusMaclearnedState
   alaDot1xDeviceStatusTimeLearned
   alaDot1xDeviceStatusCaptivePortalUsed
```

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 6450, 6350

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 ip-routing ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-security	session 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,
ip-routing      = 0x01000000 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,
domain-policy   = 0x00000000 0x000000E0,

session         = 0x00000000 0x00000100,
aaa             = 0x00000000 0x00000800,
domain-security = 0x00000000 0x00000D00


-> show aaa priv hexa rip
0x00100000 0x00000000
```

Release History

Release 6.6.1; command was introduced.

Related Commands

user	Configures or modifies user entries in the local user database.

MIB Objects

NA

aaa redirect-server

Configures redirection server name and URL details for BYOD.

aaa redirect-server *name* **hostname** *hostname* **ip-address** *ip_address* **url-list {***redirect_url1 redirect_url2 redirect_url3***}**

Syntax Definitions

name	Name of the redirection server (maximum 32 characters).
hostname	FQDN name of the Redirect Server (maximum 256 characters).
ip_address	The IPv4 address for the redirect server name.
redirect_url1	The URL list specified for the redirect server (maximum 128 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The hostname or IP address can be configured for Redirect Server
- User can assign up to 5 redirect URL names to the URL list. Assign URL links to URL names using the command **aaa redirect url**.
- A maximum of 5 URLs can be added to the redirect-server.

Examples

```
-> aaa redirect-server byod ip-address 172.26.36.26 url-list url1 url2 url3
-> aaa redirect-server upam hostname alcatel
-> aaa redirect-server upam hostname alcatel url-list url1
```

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R04; Hostname parameter added.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

aaa redirect url	Specifies the different type of URL names that are applied on the redirection UNP.
show aaa redirect-server	Displays redirection server name and its details.

MIB Objects

```
aaaRedirectServerTable
   aaaRedirectServerName
   aaaRedirectServerIpAddress
   aaaRedirectServerHostName
   aaaRedirectServerUrl1
   aaaRedirectServerUrl2
   aaaRedirectServerUrl3
   aaaRedirectServerUrl4
   aaaRedirectServerUrl5
```

aaa redirect url

Specifies the different type of URL names that are applied on the redirection UNP.

aaa redirect *name* **url {***url_name***}**

Syntax Definitions

name	Name of the redirection server (maximum 32 characters).
url_name	The URL names specified for the redirection UNP (maximum 128 characters). A maximum of 5 redirect URLs as strings.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

Assign URL names first using command **aaa redirect-server.** Then assign URL links to URL names.

Examples

```
-> aaa redirect  url url1 http://clearpassuserregistration.page
-> aaa redirect  url url2 http://clearpassuser.redirect.page
-> aaa redirect  url url3 http://clearpassbyod.main.page2
```

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

aaa redirect-server	Specifies the different type of URL names that are applied on the redirection UNP.
show aaa redirect-server	Displays redirection server name and its details.

MIB Objects

```
aaaRedirectServerTable
   aaaRedirectServerUrlName
   aaaRedirectServerUrl
```

aaa port-bounce

Enables or disables BYOD port bounce on the port, a range of ports, slots, or globally on the switch. Re-authenticates non-supplicant client to get new IP address and get full access of the network.

aaa port-bounce [*slot/port* | *slot* | *slot/port1-portn*] **{enable | disable}**

Syntax Definitions

slot	Specifies slot number on the switch.
slot/port	Specifies port number on the switch.
slot/port1-portn	Specifies a range of ports on the switch.
enable	Enables port bounce on the specified ports. If slots and ports are not specified then port bounce is enabled globally on all switch ports.
disable	Disables port bounce on the specified ports. If slots and ports are not specified then port bounce is disabled globally on all switch ports.

Defaults

By default, the global status of port bouncing is enabled.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When no slot or port number is mentioned with this command, port bouncing is enabled on all slots and ports.
- The port bouncing configuration per port can be enabled or disabled after global port bounce is enabled.
- Enable or disable option is available per-port basis using the slot or port number.

Examples

```
-> aaa port-bounce enable
-> aaa port-bounce disable
-> aaa port-bounce 1 enable
-> aaa port-bounce 2/3 enable
-> aaa port-bounce 2/4-8 enable
```

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

show aaa port-bounce status	Displays the status of global and port specific port bounce configuration.

MIB Objects

```
aaaRedirectGlobalConfigTable
   aaaPortBounceGlobalStatus
aaaPortBounceInterfaceTable
   aaaPortBouncePortSlot
   aaaPortBounceIF
```

aaa redirect pause-timer

Configures the pause timer value.

aaa redirect pause-timer *seconds*

Syntax Definitions

seconds	Indicates the pause timer value in seconds (0-65535).

Defaults

By default, the redirect pause timer value is 30.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

User-defined pause timer values must be in multiples of 5.

Examples

```
-> aaa redirect pause-timer 25
```

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

show aaa redirect pause-timer	Specifies the VLAN for the access of network with various scenarios mentioned optionally.

MIB Objects

```
aaaRedirectGlobalConfigTable
   aaaRedirectPauseTimerConfig
```

aaa redirect proxy-server-port

Configures the HTTP proxy port number to use for redirection to the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) server.

aaa redirect proxy-server-port *proxy_port*

no aaa rediret proxy-server-port

Syntax Definitions

proxy_port	The HTTP proxy port number. The valid range is 1024–49151.

Defaults

By default, the redirect proxy port number is set to 8080 (traps HTTP 80, 8080, and 443).

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the **no** form of this command to set the proxy port number back to the default (8080).
- The redirect proxy port setting only applies when a redirect server is configured for the switch.
- Configuring the switch to interact with the UPAM or CPPM is done as part of the OmniSwitch implementation of the Bring Your Own Devices (BYOD) solution.

Examples

```
-> aaa redirect proxy-server-port 8887
-> no aaa redirect proxy-server-port
```

Release History

Release 6.4.2.R02; command was introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

aaa port-bounce	Configures the port bounce action for a port or globally for the switch.
aaa redirect pause-timer	Configures the global pause timer value for the switch.
aaa redirect-server	Configures an IP network address to allow HTTP traffic redirection.

MIB Objects

```
aaaRedirectGlobalConfig
   aaaRedirectProxyServerPort
```

show aaa redirect-server

Displays redirection server name and its details.

show aaa redirect-server

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When the IP address is configured for Redirect server the hostname will be displayed as -.
- When the hostname is configured for Redirect server the IP address will be displayed as -.
- After DNS Resolution is succeeded, the IP address will be displayed.

Examples

```
-> show aaa redirect-server
Redirect Server Name               :UPAM
Redirect Server Host name          :alcatel
Redirect Server Ip Address         :192.16.23.24
RedirectURL List                   :url1
                                   url2
                                   url3
Redirect Proxy Server Port         :8080
```

output definitions

Redirect Server name	Name of redirection server.
Redirect Server Host name	FQDN name of the Redirect Server
Redirect Server Ip Address	IP address of redirection server.
RedirectUrl List	List of URL names configured on the redirect server.
Redirect Proxy Server Port	The HTTP proxy port number to use for redirection to a server.

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R02; **Redirect Proxy Server Port** field added.
Release 6.7.2.R04; **Redirect Server Host name** field added.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

aaa redirect-server	Configures a redirection server name and the URL details for BYOD.

MIB Objects

```
aaaRedirectServerTable
   aaaRedirectServerName
   aaaRedirectServerNameRedirect
   aaaRedirectServerIpAddress
   aaaRedirectServerUrl1
   aaaRedirectServerUrl2
   aaaRedirectServerUrl3
   aaaRedirectServerUrl4
   aaaRedirectServerUrl5
```

show aaa redirect url-list

Displays the different URL names applied on the redirection server. This command displays upto five user defined redirection URL names with its corresponding URL.

show aaa redirect url-list

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

When no port number is specified with the command, the global list of configured redirect URLs and URL names is displayed.

Examples

```
-> show aaa redirect url-list
URL name                    URL Address
----------------+-----------------------------------------+------
url1              http://clearpass.user.registration.page
url2              http://clearpass.user.redirect.page
url3              http://clearpass.byod.main.page
```

output definitions

URL name	Name of assigned URL.
URL Address	URL address of redirection clearpass server.

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

aaa redirect url	Specifies the different type of URL names that are applied on the redirection UNP.

MIB Objects

```
aaaRedirectUrlConfigTable
   aaaRedirectServerUrlName
   aaaRedirectServerUrlNameList
   aaaRedirectServerUrlRedirection
```

show aaa port-bounce status

Displays the status of global and port specific port bounce configuration.

show aaa port-bounce status *slot/port*

Syntax Definitions

slot/port	The port number of the port on which new BYOD devices must be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show aaa port-bounce status

Global Status       : ENABLED

Slot/port              port bounce
---------------+---------------------
1/1                      DISABLED
1/2                      ENABLED
1/3                      ENABLED
1/4                      ENABLED
1/5                      ENABLED
```

output definitions

Global Status	Global port bounce configuration Status.
Slot/port	Global list of configured ports.
port bounce	Port bounce status on slot/port basis (**ENABLED** or **DISABLED**).

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

aaa port-bounce	Enables or disables BYOD port bounce on the port, a range of ports, slots, or globally on the switch. Re-authenticates non-supplicant client to get new IP address and get full access to the network.

MIB Objects

```
aaaPortBounceInterfaceTable
   aaaRedirectGlobalConfig
   aaaPortBounceConfig
   aaaPortBounceSlotNumber
   aaaPortBouncePortNumber
```

show aaa redirect pause-timer

Displays the configured global pause-timer value.

show aaa redirect pause-timer

Syntax Definitions

N/A

Defaults

By default, the pause timer value is 30 seconds.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- On ports where port bouncing is not applied, the switch clears all authentication states on the device and pause for some period of time.
- Pause timer value must be multiples of five.

Examples

```
-> show aaa redirect pause-timer

Pause-timer value  : 120(Sec)
```

output definitions

Pause-timer value	Displays the configured pause timer value in seconds (range from 0 to 65535).

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

aaa redirect pause-timer	Specifies the different type of URL names that are applied on the redirection UNP.

MIB Objects

```
aaaRedirectGlobalConfig
   aaaRedirectPauseTimerConfig
```

show byod host

Displays the status of the new BYOD clients that come to the network.

show byod host

Syntax Definitions

slot/port	The port number of the port on which new BYOD devices must be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show byod host
Client MAC                      Status
Address
----------------------+---------------------
00:00:00:00:00:01           BYOD inprogress
00:00:00:01:07:09           BYOD complete
00:01:02:03:09:00           BYOD complete
```

output definitions

Client MAC	The new client MAC address that entered in to the network.
Status	Status of the BYOD client, either **BYOD inprogress** or **BYOD complete**.

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

aaa user-network-profile	Configures a User Network Profile (UNP) that is used to provide role-based access to the switch.

MIB Objects

```
aaaByodStatusInfoTable
   aaaByodClientmac
   aaaByodProgressStatus
```

show byod status

Displays the status of the BYOD clients at switch or per port level.

show byod status *slot/port*

Syntax Definitions

slot/port	The port number of the port on which new BYOD devices must be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show byod status 1/4

Byodconfig for slot 1 and port 4:
  Client MAC         : 00:01:02:03:09:0
  Old UNP            : UNP1
  New UNP            : validUNP
COA status           : Success BYOD complete
```

output definitions

Client MAC	The client MAC address which is newly entered in to the network.
Old UNP	Displays the old UNP assigned to the client when it is unknown MAC.
New UNP	The new UNP's VLAN assigned to the client with full network access.
COA status	Status of the client in COA/Clearpass context

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

N/A

MIB Objects

```
aaaByodConfigTable
   aaaByodConfigIntfNumber
   aaaByodClientmac
   aaaByodPreviousUNP
   aaaByodNewUNP
   aaaByodCOAStatus
```

show aaa byod white-list ip-address

Displays the status of the BYOD white list IP addresses.

show aaa byod white-list ip address

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show aaa byod white-list ip-address
IP Address              Mask
+---------------------------------------+
171.1.1.1                255.255.255.255
172.2.2.2                255.255.255.255
173.3.3.3                255.255.255.255
```

Release History

Release 6.6.5 command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

N/A

MIB Objects

```
aaaBYODWhiteListTable
   aaaBYODWhiteListIPAddress
   aaaBYODWhiteListIPMask
```

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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show aaa user-network-profile
                                        Max         Max       Max        Redirect
Role Name Vlan HIC Policy List Name Ingress-BW Egress-BW Default-Depth  URL name
----------+----+----+----------------+-----------+-----------+--------------
byodunp   100                                                          url2
check     203                                                          default-url
```

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 depth associated to UNP.
Redirect URL name	The redirection URL used to re-direct to the Clearpass page for the BYOD feature.

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R05; support for OmniSwitch 6350 added.

Related Commands

N/A

MIB Objects

```
aaaByodConfigTable
   aaaByodConfigIntfNumber
   aaaByodClientmac
   aaaByodPreviousUNP
   aaaByodNewUNP
   aaaByodCOAStatus
```

mdns-relay

Enables or disables the Multicast DNS (mDNS) relay.

mdns-relay {enable | disable}

Syntax Definitions

enable	Enables the mDNS relay.
disable	Disables the mDNS relay.

Defaults

The mDNS relay is disabled by default.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- A GRE Tunnel interface must be associated to the switch before enabling mDNS relay.
- The mDNS packets will be handled in the conventional way on disabling the mDNS relay on the switch.

Example

```
-> mdns-relay enable
-> mdns-relay disable
```

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R02; command was deprecated.

Related Commands

mdns-relay tunnel	Associates a GRE tunneling interface for the Multicast DNS (mDNS) relay.
zeroconf mdns admin-state	Enables or disables the Multicast DNS (mDNS) relay on the switch.

MIB Objects

```
mdnsSnoopingTable
   alaMdnsAdminStatus
```

mdns-relay tunnel

Associates a GRE tunneling interface for the Multicast DNS (mDNS) relay.

mdns-relay tunnel *ip interface name*

no mdns-relay tunnel *ip interface name*

Syntax Definitions

ip interface name	Name of the IP interface used by the mDNS relay for GRE tunneling. The IP interface must be created before being associated.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- A Layer 2 GRE Tunnel interface must be associated to the switch before enabling mDNS relay. Only Layer 2 GRE Tunnel interface is supported.
- GRE Tunneling is supported only for IPv4 frames.
- The IP interface name should be created before being associated. Use the **ip interface** command to create an ip interface.
- To change the GRE tunnel interface, execute the command with the new existing IP interface name.
- Using the **no** option with this command shall remove the GRE tunneling interface associated.

Example

```
-> mdns-relay tunnel Payroll
-> no mdns-relay tunnel Payroll
```

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R02; command was deprecated.

Related Commands

zeroconf mdns admin-state	Enables or disables the Multicast DNS (mDNS) relay on the switch.

MIB Objects

```
mdnsSnoopingTable
   alaMdnsGreTunnelName
```

zeroconf mdns admin-state

Enables or disables the Multicast DNS (mDNS) relay on the switch.

zeroconf mdns admin-state {enable | disable}

Syntax Definitions

enable	Enables the mDNS relay on the switch.
disable	Disables the mDNS relay on the switch.

Defaults

The mDNS relay feature is disabled by default.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

The mDNS packets will be handled in the conventional way on disabling the mDNS relay on the switch.

Example

```
-> zeroconf mdns admin-state enable
-> zeroconf mdns admin-state disable
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

zeroconf ssdp admin-state	Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.
show zeroconf config	Displays the zero configuration for the switch.

MIB Objects

`alaZeroConfMdnsAdminStatus`

zeroconf ssdp admin-state

Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch. SSDP relay enables the OmniSwitch to allow non-Apple devices to discover services with minimal configuration by the administrator.

zeroconf ssdp admin-state {enable | disable}

Syntax Definitions

enable	Enables the SSDP relay on the switch.
disable	Disables the SSDP relay on the switch.

Defaults

The SSDP relay feature is disabled by default.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The Digital Living Network Alliance (DLNA) uses Universal Plug and Play (UPnP) for media management, discovery, and control. DLNA/UPnP uses SSDP to discover services, similar to how Bonjour uses mDNS for the same. All the SSDP packets coming in on an OmniSwitch are intercepted and tunneled through the GRE tunnel to the WLAN controller (acting as a gateway).
- When SSDP relay is disabled on the switch, SSDP packets are handled in the same manner as conventional packets.

Example

```
-> zeroconf ssdp admin-state enable
-> zeroconf ssdp admin-state disable
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

zeroconf mdns admin-state	Enables or disables the Multicast DNS (mDNS) relay on the switch.
show zeroconf config	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfSsdpAdminStatus
```

zeroconf mode

Configures the mode of the SSDP or MDNS packet processing.

zeroconf mode [gateway] [tunnel [type standard]]

Syntax Definitions

gateway	The received packets are forwarded to all the VLANs in the gateway VLAN list.
tunnel	This is Aruba mode. The packets are sent to the responder through the configured GRE tunnel with protocol value of 0x0.
type standard	This is standard mode. The packets are sent to the responder through the configured GRE tunnel with protocol value of 0x6558. The packets are forwarded to all the VLANs in the access VLAN list if packet is tagged to the VLAN 4095.

Defaults

The tunnel mode (Aruba mode) is enabled by default without the type standard.

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- In tunnel mode, the responder IP address must be configured to tunnel the mDNS or SSDP packets. The mDNS operational status will be DOWN until the responder IP address is configured.
- In tunnel mode, the mDNS and SSDP packets are processed only when the Loopback0 IP address is configured as the source IP address for the tunneled packets. Use the **ip interface** command to configure the interface address.
- The switch can operate in only one mode at a time.

Example

```
-> zeroconf mode gateway
-> zeroconf mode tunnel
-> zeroconf mode tunnel type standard
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

zeroconf mdns admin-state	Enables or disables the Multicast DNS (mDNS) relay on the switch.
zeroconf ssdp admin-state	Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.
zeroconf responder-ip	Configures the IP address of the tunnel endpoint (zero configuration responder).
show zeroconf config	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfMode
   alaZeroConfTunnelMode
```

zeroconf responder-ip

Configures the IP address of the responder tunnel endpoint.

zeroconf responder-ip *ipv4address*

no zeroconf responder-ip *ipv4address*

Syntax Definitions

responder-ip	This is IP address of the zero configuration responder.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- Only IPv4 address can be configured as a responder IP address.
- In tunnel mode, the responder IP address must be configured to tunnel the mDNS or SSDP packets.
- The operational status of the mDNS or SSDP will be DOWN until the responder IP address is configured.
- The operational status of the mDNS or SSDP will be DOWN, if the configured responder IP address is not reachable.
- To remove the responder IP address configuration, use the **no** form of the command.

Example

```
-> zeroconf responder-ip 10.0.0.1
-> no zeroconf responder-ip 10.0.0.1
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

zeroconf mdns admin-state	Enables or disables the Multicast DNS (mDNS) relay on the switch.
zeroconf ssdp admin-state	Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.
zeroconf mode	Configures the mode of the SSDP or MDNS packet processing.
show zeroconf config	Displays the zero configuration for the switch.

MIB Objects

`alaZeroConfResponderIpAddr`

zeroconf gateway-vlan-list

Adds or deletes a VLAN from the gateway VLAN list.

zeroconf gateway-vlan-list *vlan-id1...vlan-idn*

no zeroconf gateway-vlan-list *vlan-id1...vlan-idn*

Syntax Definitions

vlan-id	The existing VLAN ID to be added or deleted from the gateway VLAN list. The valid range is 1-4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The gateway VLAN list can be configured only in the gateway mode.
- A maximum of 10 gateway VLANs is supported.
- To remove a VLAN from the gateway VLAN list, use the **no** form of the command.

Example

```
-> zeroconf gateway-vlan-list 1 2 4
-> no zeroconf gateway-vlan-list 4
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
show zeroconf config	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfGatewayVlanTable
   alaZeroConfGatewayVlanEntry
```

zeroconf access-vlan-list

Adds or deletes a VLAN from the access VLAN list.

zeroconf access-vlan-list *vlan-id1...vlan-idn*

no zeroconf access-vlan-list *vlan-id1...vlan-idn*

Syntax Definitions

vlan-id	The existing VLAN ID to be added or deleted from the access VLAN list. The valid range is 1-4094.

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

- The access VLAN list must be configured only in responder mode (tunnel type standard).
- The list can contain a maximum of 16 access VLANs.
- To remove a VLAN from the access VLAN list, use the **no** form of the command.

Example

```
-> zeroconf access-vlan-list 6 7 9
-> no zeroconf access-vlan-list 7
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

zeroconf mode	Configures the mode of the SSDP or mDNS packet processing.
show zeroconf config	Displays the zero configuration for the switch.

MIB Objects

```
alaZeroConfAccessVlanTable
   alaZeroConfAccessVlanEntry
```

show mdns-relay config

Displays the MDNS relay configuration.

show mdns-relay config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Example

```
-> show mdns-relay config

mdns-relay admin status    : enabled,
mdns-relay tunnel interface: tnl-MDNS
mdns-relay tunnel status   : UP
```

output definitions

mdns-relay admin status	Displays the mDNS relay feature status: enabled or disabled.
mdns-relay tunnel interface	Specifies the GRE tunnel name for the mDNS relay feature.
mdns-relay tunnel status	Displays the status of the tunnel.

Release History

Release 6.6.5; command introduced.
Release 6.7.2.R02; command was deprecated.

Related Commands

mdns-relay	Enables or disables the Multicast DNS (mDNS) relay feature.
mdns-relay tunnel	Associates a GRE tunneling interface for the Multicast DNS (mDNS) relay feature.

MIB Objects

```
mdnsSnoopingTable
   alaMdnsAdminStatus
   alaMdnsGreTunnelName
```

```
alaMdnsFloodVlans
```

show zeroconf config

Displays the zero configuration for the switch.

show zeroconf config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450

Usage Guidelines

N/A

Examples

```
-> show zeroconf config
```

Example for default mode (Aruba mode)

```
zero-conf mode          : tunnel
zero-conf tunnel type   : aruba
gre-protocol            : 0x0
MDNS admin status       : disabled
SSDP admin status       : disabled
MDNS operational status : down
SSDP operational status : down
Responder IP            : -
Tunnel Source IP        : -
```

Example for Standard mode

```
zero-conf mode          : tunnel
zero-conf tunnel type   : standard
gre-protocol            : 0x6558
MDNS admin status       : enabled
SSDP admin status       : enabled
MDNS operational status : down
SSDP operational status : down
Responder IP            : 10.0.0.1
Tunnel Source IP        : -
Access vlans list       : 1, 2, 3
```

Example for Gateway mode

```
zero-conf mode          : gateway
MDNS admin status       : enabled
SSDP admin status       : enabled
MDNS operational status : up
```

```
SSDP operational status : up
Gateway vlans list       : 4, 5, 6
```

output definitions

zero-conf mode	Displays the mode in which Zero Configuration packets is handled.
zero-conf tunnel type	Displays the type of Zero Configuration tunnel-mode. The tunnel has two types default (aruba mode) and standard mode.
gre-protocol	Displays the GRE protocol type based on the tunnel type. If tunnel is Aruba, then the GRE protocol type is 0x0. If tunnel type is Standard, then the GRE protocol type is 0x6558.
MDNS admin status	Displays the administrative status of Zero Configuration mDNS.
SSDP admin status	Displays the administrative status of Zero Configuration SSDP.
MDNS operational status	Displays the operational status of mDNS, up or down.
SSDP operational status	Displays the operational status of SSDP, up or down.
Responder IP	Displays the configured responder IP address. This is displayed only for Zero Configuration tunnel-mode.
Tunnel Source IP	Displays the configured tunnel source IP address. This is displayed only for Zero Configuration tunnel-mode.
Access vlans list	Displays the list of VLANs to which the mDNS or SSDP packets is forwarded. This is displayed only for Zero Configuration tunnel-mode type standard.
Gateway vlans list	Displays the list of VLANs to which the mDNS or SSDP packets is forwarded. This is displayed only for Zero Configuration mode type gateway.

Release History

Release 6.7.2.R02; command introduced.

Related Commands

N/A

MIB Objects

```
alaZeroConfConfig
   alaZeroConfMdnsAdminStatus
   alaZeroConfSsdpAdminStatus
   alaZeroConfMode
   alaZeroConfTunnelMode
   alaZeroConfResponderIpAddr
   alaZeroConfGatewayVlan
   alaZeroConfAccessVlan
```

aaa switch-access mode

Globally sets the access mode as enhanced or default.

aaa switch-access mode {default | enhanced}

Syntax Definitions

default	Sets the access mode as default.
enhanced	Sets the access mode as enhanced.

Defaults

parameter	default
default | enhanced	**default**

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- ASA mode is not enabled by default or when the switch is in the factory default state. The mode must first be activated through CLI through console access with default username and password (admin/ switch). However, to avoid this initial CLI command, the new mode can also be activated by creating ‘asaAdvancedMode.cfg’ file in the /flash/switch directory.
- It is recommended to save configuration and reboot the switch when the ASA mode is configured.

Example

```
-> aaa switch-access mode default
-> aaa switch-access mode enhanced
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

show aaa switch-access mode	Displays the global access mode configuration.

MIB Objects

aaaAsaAccessMode

aaa switch-access ip-lockout-threshold

Configures the threshold value for failed login attempts from an IP address after which the IP address will be banned from switch access.

aaa switch-access ip-lockout-threshold *number*

Syntax Definitions

number	Set the threshold value for login attempts in the range 0 to 999.

Defaults

parameter	default
number	6

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The command is applicable only if ASA enhanced mode is enabled.
- IP address is permanently blocked/banned if the number of authentication failures from a particular IP reaches IP lockout threshold limit.
- Only the switch access will be restricted from the banned IP address. Any IP packet (with monitored port number) destined to a switch IP interfaces will be discarded. IP packets normally bridged/routed by the switch will not be discarded.
- A maximum of 128 IP addresses can be added to the banned list. When the maximum limit has reached, oldest entry from the list is removed to accommodate the new entries.
- User lockout window (**user lockout-window**) is applicable for IP lockout threshold also.
- The IP address will remain blocked until it is released using the command **aaa switch-access banned-ip release**.

Example

```
-> aaa switch-access ip-lockout-threshold 2
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access mode	Globally sets the access mode as enhanced or default.
show aaa switch-access ip-lockout-threshold	Displays the lockout threshold configured for the remote IP addresses.

MIB Objects

```
aaaAsaIpLockoutThreshold
```

aaa switch-access banned-ip release

Releases the banned IP addresses that are blocked due to failed login attempts.

aaa switch-access banned-ip {all | *ip_address***} release**

Syntax Definitions

all	Release all banned IP addresses.
ip_address	Release a specific IP address that is banned.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

The IP addresses are banned if the failed login count reaches IP lockout threshold limit.

Example

```
-> aaa switch-access banned-ip all release
-> aaa switch-access banned-ip 100.2.45.56 release
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

show aaa switch-access banned-ip	Displays the list of banned ip addresses.

MIB Objects

```
aaaSwitchAccessBannedIpTable
   aaaSwitchAccessBannedIpAddress
   aaaSwitchAccessBannedIpRowStatus
```

aaa switch-access priv-mask

Configure the functional privileges for a particular access type.

aaa switch-access priv-mask {console | telnet | ssh | http | https} {read-only | read-write} [*families...* | *domains...*| **all | none | all-except** *families...***]**

Syntax Definitions

read-only	Specifies that the user will have read-only access to the switch through a specific access type.
read-write	Specifies that the user will have read-write access to the switch through a specific access type.
families	Determines the command families available to the user on the switch for a specific access type. 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 for a specific access type. 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 for a specific access type.
none	Specifies that no command families or domains are available to the user for a specific access type.
all-except	Specifies that functional privileges for families followed by 'all-except' are disabled for a specific access type.

Defaults

By default, the access types are enabled with read-write privileges for all the families.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The command is applicable only when ASA enhanced mode is enabled.
- The access privileges for the SSH, TELNET, Console, HTTP, HTTPS can be defined.
- 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

Example

```
-> aaa switch-access priv-mask ssh read-only webmgt vrrp vrf vlan udld
-> aaa switch-access priv-mask telnet read-write tftp-client telnet system stp ssh
-> aaa switch-access priv-mask ssh read-only all-except vlan
-> aaa switch-access priv-mask telnet read-write all-except ip
```

If privileges for specific families need to be applied, then remove the existing privilege using the **no** command, and re-apply the required family privilege.

```
-> no aaa switch-access priv-mask telnet read-write all
-> aaa switch-access priv-mask telnet read-write vlan aaa
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access mode	Globally sets the access mode as enhanced or default.
show aaa switch-access priv-mask	Displays the privilege details for the access types.

MIB Objects

```
aaaSwitchAccessPrivMaskTable
   aaaSwitchAccessType
   aaaSwitchAccessReadRight1
   aaaSwitchAccessReadRight2
   aaaSwitchAccessWriteRight1
   aaaSwitchAccessWriteRight2
   aaaSwitchAccessPrivMaskRowStatus
```

aaa switch-access management-stations

Enables or disables the IP management station feature in a switch.

aaa switch-access management-stations {enable | disable}

Syntax Definitions

enable	Enables the IP management station feature in the switch.
disable	Disables the IP management station feature in the switch.

Defaults

The IP management station feature is disabled by default.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The command is applicable only when ASA enhanced mode is enabled.
- When the IP management station is disabled, switch access from any IP address shall be allowed. If there is a login failure (based on the **ip-lockout threshold** value), the IP address will be banned/ blocked and added to the banned IP address list.
- When the IP management station is enabled, the switch access will be allowed only from those IPs configured in the management station list and only if those are not in banned list.

Example

```
-> aaa switch-access management stations enable
-> aaa switch-access management stations disable
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access mode	Globally sets the access mode as enhanced or default.
aaa switch-access management-stations ip-address	Configure the management station in the switch, with or without mask value for the corresponding IP of the management station.
show aaa switch-access management-stations	Displays the list of configured management stations.

MIB Objects

```
aaaSwitchAccessMgmtStationTable
   aaaSwitchAccessMgmtStationIpAddress
```

```
aaaSwitchAccessMgmtStationIpAddress
```

aaa switch-access management-stations ip-address

Configure the management station in the switch, with or without mask value for the corresponding IP of the management station. The remote access is allowed only from these IP addresses if management station feature is enabled.

aaa switch-access management-stations *ip_address* [**mask** *mask*]

no aaa switch-access management-stations *ip_address*

Syntax Definitions

ip_address	IP address of the management station.
mask	The mask corresponding to the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- A maximum of 64 management stations can be configured.
- Removing an IP address from the management station list will not remove the IP from the banned list as IPs which are not in the management table are blocked by default.
- Whenever an IP address is removed from the management station, switch will stop responding to that IP. However, the existing sessions are not terminated automatically.

Example

```
-> aaa switch-access management stations 100.15.9.8
-> aaa switch-access management stations 100.15.9.9 mask 255.255.255.0
```

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access management-stations	Enables or disables the IP management station feature in a switch.
show aaa switch-access management-stations	Displays the list of configured management stations.

MIB Objects

```
aaaSwitchAccessMgmtStationTable
   aaaSwitchAccessMgmtStationIpAddress
   aaaSwitchAccessMgmtStationRowStatus
```

show aaa switch-access mode

Displays the access mode configuration.

show aaa switch-access mode

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Example

```
-> show aaa switch-access mode
aaa switch-access mode: Enhanced
```

output definitions

AAA switch-access mode	ASA access mode: Enhanced or Default

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access mode	Globally sets the access mode as enhanced or default.

MIB Objects

aaaAsaAccessMode

show aaa switch-access ip-lockout-threshold

Displays the IP lockout threshold value.

show aaa switch-access ip-lockout-threshold

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Example

```
-> show aaa switch-access ip-lockout-threshold
ip lockout threshold: 6
```

output definitions

IP lockout threshold	The IP lockout threshold value.

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access ip-lockout-threshold	Configures the threshold for failed login attempts from an IP address after which the IP address will be banned from switch access.

MIB Objects

```
aaaAsaIpLockoutThreshold
```

show aaa switch-access banned-ip

Displays the list of banned IP addresses.

show aaa switch-access banned-ip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Example

```
-> show aaa switch-access banned-ip
   Sl.no       IP address
|---------+----------------|
     1       100.15.5.21
     2       100.15.5.22
```

output definitions

IP address	The banned IP address blocked due to failed login attempts.

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access banned-ip release	Releases the banned IP addresses that are blocked due to failed login attempts.

MIB Objects

```
aaaAsaIpLockoutThreshold
```

show aaa switch-access priv-mask

Displays the privilege details for the access types.

show aaa switch-access priv-mask

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show aaa switch-access priv-mask
  Access type = CONSOLE,
  Read Only for domains   = None,
  Read/Write for domains  = All

  Access type = TELNET,
  Read Only for domains   = None,
  Read/Write for domains  = All

  Access type = HTTP,
  Read Only for domains   = All ,
  Read/Write for domains  = None

  Access type = SSH,
  Read Only for domains   = None,
  Read/Write for domains  = All

  Access type = HTTPS,
  Read Only for domains   = None,
  Read/Write for domains  = All
```

output definitions

Access type	The access type.
Read Only for domains	Read-only privileges for the domains.
Read/Write for domains	Read-write privileges for the domains.

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access priv-mask	Configure the functional privileges for a particular access type.

MIB Objects

```
aaaSwitchAccessPrivMaskTable
   aaaSwitchAccessType
   aaaSwitchAccessReadRight1
   aaaSwitchAccessReadRight2
   aaaSwitchAccessWriteRight1
   aaaSwitchAccessWriteRight2
   aaaSwitchAccessPrivMaskRowStatus
```

show aaa switch-access management-stations

Displays the list of configured management stations.

show aaa switch-access management-stations

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show aaa switch-access management-stations
MANAGEMENT STATION FEATURE STATUS: ENABLED
   Sl.no       IP address       Mask
|---------+-----------------+-----------------|
 1            100.15.5.21    255.255.255.255
```

output definitions

Management Station Feature Status	IP management station status: Enabled or disabled.
IP address	IP address of the management station.
Mask	The mask corresponding to the IP address.

Release History

Release 6.7.1 R02; command introduced.

Related Commands

aaa switch-access management-stations	Enables or disables the IP management station feature in a switch.
aaa switch-access management-stations ip-address	Configure the management station in the switch, with or without mask value for the corresponding IP of the management station

MIB Objects

```
aaaSwitchAccessMgmtStationTable
   aaaSwitchAccessMgmtStationIpAddress
```

```
aaaSwitchAccessMgmtStationIpAddress
```

50 802.1x 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** **802.1x captive-portal address** **802.1x delay-learning** **802.1x auth-server-down** **802.1x auth-server-down policy** **802.1x server-polling** **802.1x trust-radius** **802.1x non-supplicant session timeout** **show 802.1x** **show 802.1x users** **show 802.1x ap-client-mac** **show 802.1x statistics** **show 802.1x non-supplicant** **show 802.1x auth-server-down** **show 802.1x rate-limit**
Access Guardian commands	**802.1x supplicant bypass** **802.1x non-supplicant allow-eap** **802.1x pass-through** **802.1x supplicant policy authentication** **802.1x non-supplicant policy authentication** **802.1x captive-portal name** **802.1x non-supplicant policy** **802.1x policy default** **802.1x captive-portal policy authentication** **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 delay-learning** **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 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 control the port control status dynamically 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 does not accept an 802.1x authentication attempt; the timer is activated after any authentication failure. During the time period specified, the switch ignores and discard all Extensible Authentication Protocol over LAN (EAPOL) packets. The range is 0 seconds to 65535 seconds.
tx-period *seconds*	The time before an EAP Request Identity is retransmitted. The range is 1 second to 65535 seconds.
supp-timeout *seconds*	The number of seconds before the switch times out an 802.1x user who is attempting to authenticate. The value must be modified to be a greater value if the authentication process requires 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 retransmits a request for authentication information (request identity, password, challenge, and so on.) 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 reauthentication of the Supplicant on this port. Only applicable when reauthentication is enabled.

reauthentication	Specifies that the port is reauthenticated after the **re-authperiod** timer expires.
no reauthentication	Specifies that the port is not 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	disabled
re-authperiod *seconds*	3600
reauthentication	disabled
reauthentication | no reauthentication	no reauthentication

Platforms Supported

OmniSwitch 6450, 6350

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 only process 802.1x frames (EAPoL frames) from an unknown source.
- 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 3/1 quiet-period 30
```

Release History

Release 6.6.1; command 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.
show 802.1x	Displays information about ports configured for 802.1x.

MIB Objects

```
dot1xPaePortTable
   dot1xPaePortNumber
   dot1xPaePortInitialize
   dot1xPaePortReauthenticate
dot1xAuthConfigTable
   dot1xAuthAdminControlledDirections
   dot1xAuthOperControlledDirections
   dot1xAuthAuthControlledPortStatus
   dot1xAuthAuthControlledPortControl
   dot1xAuthQuitePeriod
   dot1xAuthTxPeriod
   dot1xAuthSuppTimeout
   dot1xAuthServerTimeout
   dot1xAuthMaxReq
   dot1xAuthReAuthPeriod
   dot1xAuthReAuthEnabled
```

802.1x initialize

Reinitializes a particular 802.1x port. Stops traffic on the port; then requires reauthentication 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 6450, 6350

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 reauthenticated. Connectivity is restored with successful reauthentication.

Examples

```
-> 802.1x initialize 3/1
```

Release History

Release 6.6.1; command 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 reauthenticated.

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 reauthentication. Use the **802.1x re-authenticate** command to force a reauthentication.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- This command forces a port to be reauthenticated, regardless of the reauthentication setting configured for the **802.1x** command.
- Reauthentication 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 reauthentication 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 6.6.1; command 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 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 6450, 6350

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, reauthentication does 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 6.6.1; command 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-802.1x supplicants learned on one or more 802.1x ports. Displays a list of all non-802.1x supplicants learned on one or more 802.1x ports.

MIB Objects

```
alaDot1xSuppPollingCnt
```

802.1x supplicant policy authentication

Configures a supplicant device classification policy for an 802.1x port. This type of policy uses 802.1x authentication through 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 | mac-authentication}...]**

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.
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 access on the 802.1x port.
captive-portal	Use Captive Portal for web-based device classification.
mac-authentication	When 802.1x supplicant authentication fails, the failed 802.1x supplicant users are authenticated using the non-supplicant MAC authentication.

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 6450, 6350

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 (for example, **802.1x 1/10 supplicant authentication**), the resulting policy blocks supplicants if successful 802.1x authentication *does not* return a VLAN ID, returns a VLAN ID that does not exist, or authentication fails.
- When multiple parameters are configured, the policy is referred to as a compound supplicant policy. Such policies use the **pass** and **fail** parameters to specify which policies to use when 802.1x authentication is successful and which to use when it fails.
- The **pass** keyword is implied and therefore an optional keyword. If the **fail** keyword is not used, the default action is to block the device when authentication fails.
- The order in which parameters are specified determines the order in which they are applied. However, this type of policy must end with either the **default-vlan** or **block**, 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, 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.

Note. Default VLAN of the port must be different from that of the UNP VLAN. UNP Policy list is not applied with UNP classified to UNP VLAN if it is same as the default VLAN assigned to the port.

- 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.
- When the fail policy is set to MAC Authentication, the failed supplicant users will be classified based on non supplicant mac-authentication policy. After authentication, the users get classified based on the returned VLAN or based on local authorization on non supplicant policy.

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
-> 802.1x 3/1 supplicant policy authentication fail mac-authentication
```

Release History

Release 6.6.1; command introduced.
Release 6.7.1 R03; **mac-authentication** parameter 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.

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 through 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 6450, 6350

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.
- MAC-authentication is referred as non-supplicant authentication. The administrator can configure the client MAC address as the password and username in the authentication server. The MAC address of the client, to authenticate the non-supplicant, can be either in uppercase or lowercase letters.
- 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 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 policy that may 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 6.6.1; command introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server with different options for Authenticated Switch Access or 802.1X port access control.
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 captive-portal name

Configures the name of the redirect 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 6450

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 6.6.3; command introduced.

Related Commands

show 802.1x captive-portal configuration	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xCPortalRedirectString
```

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 6450, 6350

Usage Guidelines

- Because this policy does not use 802.1x or MAC authentication, non-supplicants are only classified for assignment to non-authenticated VLANs.
- 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 default-vlan
-> 802.1x 5/10 non-supplicant policy vlan 500 block
-> 8022.1x 6/1 non-supplicant policy group-mobility vlan 247 block
-> 802.1x 4/10 non-supplicant policy captive-portal
-> 802.1x 6/1 non-supplicant policy user-network-profile
```

Release History

Release 6.6.1; command introduced.

Related Commands

802.1x supplicant policy authentication	Configures 802.1x authentication device classification policies for supplicants.
802.1x non-supplicant policy authentication	Configures MAC authentication device classification policies for non-supplicants.
802.1x policy default	Resets the device classification policy to the default policy value for the 802.1x port.
show 802.1x device classification policies	Displays device classification policies configured for an 802.1x port.
show 802.1x non-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 6450, 6350

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 6.6.1; command 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 classifies both supplicants and non-supplicants that have attempted network access using 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 | user-network-profile** *profile_name* **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 6450

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 6.6.1; command 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 auth-server-down	Displays the Captive Portal configuration information (session time limit and the number of login retries) for the specified 802.1x port.

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 6450

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 6.6.1; command 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 auth-server-down	Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xCaptivePortalSessionLimit
```

802.1x captive-portal inactivity-logout

Configures whether 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 6450

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 6.6.3; command 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 6450

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 6.6.1; command 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 auth-server-down	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

ip_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 6450

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. 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 6.6.1; command introduced.

Related Commands

show 802.1x auth-server-down Displays the global Captive Portal configuration for the switch.

MIB Objects

```
alaDot1xCportalConfig
   alaDot1xCPortalIpAddress
```

802.1x delay-learning

Delays the 802.1x authentication process for the set interval after the switch reboot. Configuring the delay interval avoids the 802.1x clients from getting into the auth server down state by attempting an early authentication before the switch is rebooted.

802.1x delay-learning *num*

Syntax Definitions

integer	This is the time interval in seconds that is sent to all NIs for delaying the authentication process after reboot. The range is from 0 to 4294967295.

Defaults

By default, the delay time interval is set to 120 seconds.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to delay the authentication process when the switch is rebooted.
- The modified time interval is applied only during the next reboot of the switch.
- The configured delay learning interval can be verified using the **show 802.1x auth-server-down** command.

Examples

```
-> 802.1x delay-learning 100
```

Release History

Release 6.7.1 R03; command introduced.

Related Commands

show 802.1x auth-server-down	Displays the configured authentication server down classification policy.

MIB Objects

```
alaDot1xDelayLearningPeriod
```

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

By default, the proxy server URL value is set to **proxy**. Captive Portal looks for the word “proxy” to identify the users web server URL.

Platforms Supported

OmniSwitch 6450

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.

Examples

```
-> 802.1x captive-portal proxy-server-url www.companyname.com
```

Release History

Release 6.6.1; command introduced.

Related Commands

show 802.1x auth-server-down 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 6450

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 6.6.3; command 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 accepts and replies.

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 looks 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 6450

Usage Guidelines

- The DNS strings configured with this command are added to the list of the pre-defined DNS strings, as shown above. The pre-defined strings are not configurable and always remains 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 6.6.3; command 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 6450

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 6.6.3; command 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 6450

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 6.6.3; command 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 6450, 6350

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 6.6.2; command 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 6450, 6350

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 6.6.3; command introduced.

Related Commands

802.1x auth-server-down	Enables or disables the authentication server down policy.
show 802.1x	Configures the amount of time to wait before reauthentication 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

```
alaDot1xAuthSvrTimeoutPolicy
```

802.1x auth-server-down re-authperiod

Configures the amount of time to wait before reauthentication 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 reauthentication timer. The range is 30 second to 43200 seconds.

Defaults

parameter	default
value	30

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.2; command introduced.
Release 6.7.2.R03; Reauthentication timer increased from 9999 to 43200.

Related Commands

802.1x auth-server-down policy Configures the authentication server down policy.

show 802.1x auth-server-down Displays the configured reauthentication time interval value.

MIB Objects

```
alaDot1xAuthSvrTimeoutReAuthPeriod
```

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 6450, 6350

Usage Guidelines

- Use this command to enable or disable the authentication server down policy.
- This command is global and applies to all ports on the switch.

Examples

```
-> 802.1x auth-server-down enable
-> 802.1x auth-server-down disable
```

Release History

Release 6.6.2; command 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 the device when the authentication server is not reachable.

802.1x auth-server-down [[no] voice-policy] [policy] {user-network-profile *profile_name* **| block}**

802.1x auth-server-down no voice-policy

Syntax Definitions

profile_name	The name of an existing User Network Profile (UNP) to use for device classification.
block	Blocks supplicant access on the 802.1x port.
voice-policy	Classifies the IP phone traffic from the data traffic when the authentication server is down.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use this command to configure the authentication server down classification policy.
- Use the optional parameter **block** to restrict the device traffic on the 802.1x port.
- Use the optional parameter **voice-policy** to configure the UNP to classify IP phone traffic from the data traffic when the authentication server is down. This can be configured for POE IP phones which supports LLDP-MED.
- The **voice-policy** parameter will work only if the **802.1x auth-server-down** functionality is enabled.
- Use the **no** form of the command to remove the **voice-policy** configuration.
- This command is global and applies to all ports on the switch.
- To obtain the RADIUS server status periodically, enable the server polling using the **802.1x server-polling** command. Use **show aaa server** command to view the server status.

Examples

```
-> 802.1x auth-server-down policy user-network-profile
-> 802.1x auth-server-down policy block
-> 802.1x auth-server-down voice-policy user-network-profile UNP1
-> 802.1x auth-server-down no voice-policy user-network-profile
```

Release History

Release 6.6.2; command introduced.
Release 6.7.1; **voice-policy** parameter included.

Related Commands

show 802.1x auth-server-down	Displays the configured authentication server down classification policy.

MIB Objects

```
alaDot1xAuthServerTimeoutPolicy
alaDot1xAuthSvrTimeoutVoicePolicy
```

802.1x server-polling

Enable or disable server polling feature, which polls all the configured RADIUS servers periodically to obtain the server status.

802.1x server-polling {enable | disable}

Syntax Definitions

enable	Enables the polling of the RADIUS server.
disable	Disables the polling of the RADIUS server.

Defaults

By default, RADIUS server polling is disabled.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guideline

show aaa server command displays the reachability status of different RADIUS servers configured on the switch.

Examples

```
-> 802.1x server-polling enable
-> 802.1x server-polling disable
```

Release History

Release 6.7.1 R02; command introduced.
Release 6.7.1 R03; command deprecated. use **aaa radius-health-check** command.

Related Commands

802.1x auth-server-down policy	Configures the policy for classifying the device when the authentication server is not reachable.

MIB Objects

```
alaDot1xAuthSvrPollingStatus
```

802.1x trust-radius

Specifies whether to use the session timeout attribute value for the reauthentication time interval or to use the locally configured re-authentication time interval value.

802.1x *slot/port* **trust-radius {enable | disable}**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
enable	Enables 802.1x port to use the session-timeout attribute value for re-authentication time interval or to use the locally configured re-authentication time interval value.
disable	Disables 802.1x port to use the session timeout attribute value for re-authentication time interval.

Defaults

The default value of trust-radius parameter is disable.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Trust radius specifies whether the re-authentication interval should be taken from the session-timeout attribute of Access-Accept message returned by the RADIUS server.
- The trust-radius option is disabled by default for 802.1x authentication.
- When the trust-radius option is enabled, the timeout value returned in session-timeout attribute of Access-Accept message takes precedence over the configured re-authentication interval.
- If reauthentication is disabled, then there is no effect for the trust-radius parameter.
- The change in re-authentication interval takes effect immediately for all users that are authenticated after the configuration. For users who are already authenticated, the re-authentication interval takes effect only after the user is flushed out or when the user is re-authenticated again.

Examples

```
-> 802.1x 1/1 trust-radius enable
-> 802.1x 1/1 trust-radius disable
```

Release History

Release 6.7.2.R02; command introduced.

Related Commands

802.1x	Configures 802.1x parameters on a particular slot/port.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xSuppTrustRadiusEnabled
```

802.1x non-supplicant session timeout

Enable or disable the session timeout and set the session timeout interval for MAC authenticated users.

802.1x *slot/port* **non-supplicant session-timeout {enable | disable} [interval** *num]* **[trust-radius {enable | disable}] [inactivity-logout {enable | disable}]**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
num	Specifies the MAC session timeout in seconds.
trust-radius	Specifies whether the session timeout should be taken from the Session-Timeout attribute of Access-Accept message returned by the RADIUS server.
Inactivity-logout	Specifies if the non-supplicant MAC address must be flushed or not flushed when the MAC aging timeout happens.

Defaults

parameter	default
session-timeout	disable
Interval num	43200 seconds (12hrs)
trust-radius	disable
Inactivity-logout	enable

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The 802.1x non-supplicant session timeout is disabled by default and when enabled the default session timeout interval is set to 43200 seconds.
- The allowed range for session timeout interval is between 12000 to 86400 seconds.
- The trust-radius option is disabled by default for MAC authenticated users.
- If the session timeout is disabled, there is no effect for the interval that is configured in the command and there is no effect even if the trust-radius parameter is enabled.
- When the trust-radius option is enabled, the timeout value returned in session-timeout attribute of Access-Accept message takes precedence over the configured session-timeout.
- The change in session timeout interval takes effect immediately for all users that are authenticated after the configuration. For users who are already authenticated the session timeout interval takes effect only after the user is flushed out or when the user is re-authenticated again.

- If the inactivity-logout is disabled then MAC entry would be re-programmed in the switch after MAC aging without any re-authentication initiated by the switch. If the inactivity logout is enabled the MAC will get flushed out after MAC aging.

Examples

```
-> 802.1x 1/1 non-supplicant session-timeout enable interval 13000
-> 802.1x 1/1 non-supplicant session-timeout enable interval 14000 trust-radius
enable
-> 802.1x 1/1 non-supplicant session-timeout enable trust-radius enable
-> 802.1x 1/1 non-supplicant session-timeout disable
-> 802.1x 1/1 non-supplicant inactivity-logout disable
```

Release History

Release 6.7.2.R02; command introduced.
Release 6.7.2.R04; **inactivity-logout** parameter added.

Related Commands

802.1x	Configures 802.1x parameters on a particular slot/port.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xNonSuppSessTimeoutStatus
   alaDot1xNonSuppSessTimeoutIntrvl
   alaDot1xNonSuppSessTimeoutTrustRadStatus
   alaDot1xNonSupInactivityLogout
```

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 6450, 6350

Usage Guidelines

If you do not specify a particular slot/port, information for all 802.1x ports is displayed.

Examples

```
-> show 802.1x 1/10

802.1x configuration for slot 1 port 10:

  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)            = 30,
  reauthentication                   = yes,
  Trust-Radius                       = enabled,
  isPortAP                           = yes,
  Supplicant polling retry count     = 2,
  Captive Portal Session Limit (hrs) = 12,
  Captive Portal Login Retry Count   = 3,
  Supplicant Bypass                  = disable,
  Supplicant Bypass allow-eap Branch = none,
  Non-Supp reauthentication          = disabled,
  Non-Supp re-authperiod (seconds)   = 43200,
  Non-Supp Trust-Radius              = disabled,
  Non-Supp InactivityLogout          = disabled,
  Captive Portal Inactivity Logout    = Disabled,
```

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 MAC address of the port becomes operable. If the MAC address of the port 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 does not accept an 802.1x authentication attempt; the timer is activated after any authentication failure. The range is 0 seconds to 65535 seconds. Configured through the **802.1x** command.
tx-period	The time before an EAP Request Identity is transmitted. The range is 1 second to 65535 seconds. Configured through the **802.1x** command.
supp-timeout	The number of seconds before the switch times 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 retransmits a request for authentication information (request identity, password, challenge, and so on.) 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 reauthentication of the Supplicant on this port. Only applicable when reauthentication is enabled. Configured through the **802.1x** command.
reauthentication	Whether the port is reauthenticated after the re-authperiod expires. Configured through the **802.1x** command.
Trust-Radius	The trust RADIUS status (**enabled** or **disabled**). When enabled, the timeout value returned in the session-timeout attribute of an Access-Accept message is displayed. When disabled, the locally configured re-authentication timeout value is displayed. Configured through the **802.1x trust-radius** command.
isPortAP	Whether the device connected to the 802.1x port is an OmniAccess Stellar Access Point (AP).
Supplicant polling retry count	The number of times a device is polled for EAP frames to determine whether the device is an 802.1x client. Configured through the **802.1x supp-polling retry** command.

output definitions (continued)

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.
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**.
Non-Supp reauthentication	Whether the port is reauthenticated after the re-authperiod expires. Configured through the **802.1x** command.
Non-Supp re-authperiod	The amount of time that must expire before the switch requires reauthentication of the Non-Supplicant on this port. Only applicable when reauthentication is enabled. Configured through the **802.1x** command.
Non-Supp Trust-Radius	The trust RADIUS status (**enabled** or **disabled**). When enabled, the timeout value returned in the Session-Timeout attribute of Access-Accept message is displayed. When disabled, the locally configured re-authentication timeout value is displayed. Configured through the **802.1x non-supplicant session timeout** command.
Non-Supp InactivityLogout	The inactivity-logout status (**enabled** or **disabled**). When enabled, the MAC address will be flushed else it will be re-programmed to the switch.
Captive Portal Inactivity Logout	Whether 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.

Release History

Release 6.6.3; command introduced.
Release 6.7.2.R02; **isPortAP**, **Trust-Radius**, and **Non-Supp Trust-Radius** fields added.
Release 6.7.2.R04; **Non-Supp InactivityLogout** field 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
alaDot1xAuthPolicyEntry
   alaDot1xNonSuppSessTimeoutStatus
   alaDot1xNonSuppSessTimeoutIntrvl
   alaDot1xNonSuppSessTimeoutTrustRadStatus
   alaDot1xSuppTrustRadiusEnabled
   alaDot1xNonSupInactivityLogout
```

show 802.1x users

Displays a list of all users for one or more 802.1x ports.

show 802.1x users [*slot/port***]**

Syntax Definitions

slot	The slot of the port for which you want to display information.
port	The port for which you want to display 802.1x information.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- If you do not specify a particular slot/port, all users associated with 802.1x ports are displayed.
- If the session-timeout is disabled for MAC/non-supplicant users and if the re-authentication is disabled for 802.1x/supplicant users, then the ReAuthPeriod Value in the show command will display the timer value in which the user authenticated last time.

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 01:36:24 2075   user

   -> show 802.1x users detail
   Slot/Port                 = 02/13
     MAC Address             = 00:00:c3:de:79:b8
     Port State              = Authenticated
     Classification Policy   = Basic-VLAN ID
     VLAN Learned            = 100
     Username                = Admin9999
     ReAuthPeriod            = 60
     Dynamic UNP             = Disabled
     HIC Status              = Not Started
```

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.
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.
Auth Failure Reason	Displays the reason for authentication failure.
Auth Retry Count	Displays the number of times the switch re-transmitted a request to the 802.1x user for authentication information.
Last Successful Auth Time	Displays the latest successful authentication time.
User Name	The user name that is used for authentication.

Release History

Release 6.6.1; command introduced.
Release 6.6.3; **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
   alaDot1xPortVlan
   alaDot1xPortProtocol
alaDot1xAuthPolicyTable
   alaDot1xSuppPolicy
   alaDot1xSupplicantPolicyUs
   alaDot1xNonSuppPolicy
```

show 802.1x ap-client-mac

Displays all the wireless client MAC addresses received on an 802.1X port that is connected to an OmniAccess Stellar Access Point (AP).

show 802.1x ap-client-mac *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 6450, 6350

Usage Guidelines

Only the MAC addresses of Stellar AP wireless clients learned on 802.1x ports are displayed.

Examples

```
-> show 802.1x AP-client-mac
Slot  MAC               Vlan
Port  Address           Learned
-----+-----------------+-----------
1/1   00:00:c3:de:79:b8 200
      00:00:c3:de:80:b1 210
1/20  00:00:c3:d3:81:c1 300
      00:00:c3:d3:82:c2 310

-> show 802.1x AP-client-mac 1/1
Slot  MAC               Vlan
Port  Address           Learned
-----+-----------------+-----------
1/1   00:00:c3:de:79:b8 200
      00:00:c3:de:80:b1 210
```

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.
Vlan Learned	The VLAN ID on which the AP client MAC address was learned. This corresponds with the VLAN tag of the learned client traffic.

Release History

Release 6.7.2.R02; command introduced.

Related Commands

show 802.1x	Displays the 802.1x configuration for one or more ports.

MIB Objects

N/A

show 802.1x statistics

Displays statistics about all 802.1x ports or for a particular 802.1x port.

show 802.1x statistics [*slot/port***]**

Syntax Definitions

slot	The slot of the port for which you want to display 802.1x statistics.
port	The port for which you want to display 802.1x statistics.

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; command 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 6450, 6350

Usage Guidelines

Use the *slot/port* parameter to display device classification policies for a specific 802.1x port.

Examples

```
-> show 802.1x device classification policies
Device classification policies on 802.1x port 2/26
 Supplicant:
    authentication, block
 Non-Supplicant:
    block
Device classification policies on 802.1x port 2/47
 Supplicant:
    authentication, block
 Non-Supplicant:
    block
Device classification policies on 802.1x port 2/48
 Supplicant:
    authentication, vlan  247, default-vlan
 Non-Supplicant:
    authentication:
       pass: group-mobility, block
       fail: strict-vlan  347, default-vlan

-> show 802.1x device classification policies 2/48
Device classification policies on 802.1x port 2/48
 Supplicant:
    authentication, vlan  247, default-vlan
 Non-Supplicant:
    authentication:
       pass: group-mobility, block
       fail: strict-vlan  347, default-vlan
-> show 802.1x device classification policies 2/2
Device classification policies on 802.1x port 2/2
```

```
Supplicant:
    authentication:
       pass: group-mobility, UNP unp, default-vlan
       fail: UNP unp, mac-authentication
Non-Supplicant:
    authentication:
       pass: default-vlan
       fail: block
Captive Portal:
    authentication:
       pass: default-vlan
       fail: block
```

output definitions

Supplicant:	Displays the supplicant device classification policy configured for the 802.1x port.
Non-Supplicant:	Displays the non-supplicant device classification policy configured for the 802.1x port.

Release History

Release 6.6.1; command introduced.
Release 6.7.1 R03; **mac-authentication** fail policy included in show output.

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 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 6450

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 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 delay-learning** 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 6.6.3; command introduced.

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
```

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***]**

Syntax Definitions

slot/port	The slot/port number of the 802.1x port for which you want to display information.

Defaults

All non-supplicants associated with all 802.1x ports are displayed.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the *slot/port* parameter to display a list of non-supplicants learned on a specific 802.1x port.
- If trust-radius option is enabled, the session-timeout attribute value received from the server in an access accept message will be displayed. If trust radius option is disabled, the locally configured re-authentication timer value will be displayed.

Examples

```
-> show 802.1x non-supplicant
Slot  MAC               MAC Authent      Classification    Vlan      User
Port  Address           Status           Policy            Learned   Name
-----+------------------+--------------+-----------------+--------+------------
01/13 00:00:00:00:2c:83  Authenticated   Basic-GM           10      000000002c83
01/13 00:00:00:00:3c:82 Authenticated   Basic-GM           10      000000003c82
02/10 00:00:00:00:7c:86 Authenticated   Basic-GM           10      000000007c86

-> show 802.1x non-supplicant detail
Slot/Port                = 01/13
  MAC Address            = 00:00:00:00:2c:83
  MAC Authen Status      = Authenticated
  Classification Policy  = Basic-GM
  VLAN Learned           = 10
  Dynamic UNP            = Disabled
  UserName               = 000000002c83
  ReAuthPeriod           = 40
  HIC Status             = Not Started

-> show 802.1x non-supplicant unp
Slot  MAC               Vlan  HIC             Dynamic   User
Port  Address                 Status          UNP       Name
-----+-----------------+-----+---------------+-------+-------------
03/01 00:00:00:00:00:01    10 Not Started     unp     000000000001
```

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.
Authentication Status	Indicates the MAC authentication status. • **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.
User Name	Displays the user-name entered through MAC authentication, if the user is a MAC user.

Release History

Release 6.6.1; command introduced.
Release 6.7.2; User Name parameter added in the show command display.

Related Commands

show 802.1x	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
```

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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> show 802.1x auth-server-down

Status                      = Enabled
Re-authentication Interval = 900 seconds
Delay-Learning Period      = 300 seconds
Classification policy        = UNP 'unp', block
Classification Voice Policy  = None

-> show 802.1x auth-server-down

Status                         = Disabled
Re-authentication Interval    = 30 seconds
Delay-Learning Period          = 120 seconds
Classification policy          = UNP 'unp1', block
Classification Voice Policy    = UNP 'unp2'
```

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 it is classified according to the Auth-server-policy.
Delay-Learning Period	It is the time interval that is sent to all NIs for delaying the authentication process after reboot.
Classification Policy	The 802.1x device classification policy that was applied to the device.
Classification Voice Policy	Displays the UNP for which the voice policy is configured. If Voice Policy is not configured, “None” is displayed.

Release History

Release 6.6.2; command introduced.
Release 6.7.1; **Classification Voice Policy** output field included.
Release 6.7.1 R03; **Delay-Learning Period** output field included.

Related Commands

802.1x auth-server-down	Enables or disables the authentication server down policy.
802.1x auth-server-down policy	Configures the policy for classifying the device when the authentication server is not reachable
802.1x delay-learning	Delays the 802.1x authentication process for the set interval after the switch reboot.
show 802.1x	Configures the reauthentication time for the device to authenticate again with the RADIUS server when it is classified according to the Auth-server-down policy

MIB Objects

N/A

show 802.1x rate-limit

Displays the current rate limit configuration on 802.1x enabled ports. If a port is not specified, then current rate limit configuration for all 802.1x 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 6450, 6350

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 802.1x 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 802.1x 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 802.1x 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 6.6.4; command introduced.

Related Commands

802.1x	Configures 802.1x parameters on a particular slot/port.

MIB Objects

```
alaDot1xCrlUnpTable
   alaDot1xCrlSlotNumber
   alaDot1xCrlPortNumber
   alaDot1xCrlIngBw
   alaDot1xCrlIngTypeFlag
   alaDot1xCrlIngProfile
   alaDot1xCrlEgrBw
   alaDot1xCrlEgrTypeFlag
   alaDot1xCrlEgrProfile
```

802.1x supplicant bypass

Configures whether 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 performed first.

Defaults

By default, supplicant bypass is disabled; 802.1x authentication is performed first.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use 802.1x supplicant bypass command with the **802.1x non-supplicant allow-eap** command to initiate MAC authentication on any device, and to specify whether subsequent 802.1x authentication is also performed on the same device depending on the MAC authentication outcome and allow-eap configuration.
- 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 frees up those devices to undergo the authentication specified by the new bypass configuration.
- If reauthentication 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 reauthentication 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 6.6.3; command introduced.

Related Commands

802.1x	Configures 802.1x parameters for the specified port.
802.1x non-supplicant allow-eap	Configures whether 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 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

Default value is ‘none’. Only MAC authentication is applied to the supplicant device (802.1x classification is not performed on the supplicant device).

Platforms Supported

OmniSwitch 6450, 6350

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 does 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 6.6.3; command 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 forward 802.1x EAP frames transparently.

802.1x pass-through {enable | disable}

Syntax Definitions

slot/port	The slot and port number of the 802.1x port.
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 6450, 6350

Usage Guidelines

- Use this command to globally set the switch to forward 802.1x EAP frames transparently.
- Pass through mode must be enabled on the layer2 switch to allow EAP packets to be trapped on the Layer3 switch for authentication.

Examples

```
-> 802.1x pass-through enable
-> 802.1x pass-through disable
```

Release History

Release 6.6.3; command introduced.

Related Commands

802.1x	Configures 802.1x parameters for the specified port.
show 802.1x	Displays the 802.1x configuration for the port.

MIB Objects

```
alaDot1xPassThroughStatus
```

show 802.1x captive-portal configuration

Displays the Captive Portal configuration information (session time limit and the number of login retries) for the specified 802.1x port.

show 802.1x captive-portal configuration [*slot/port***]**

Syntax Definitions

slot/port	The slot and port number of the 802.1x port for which you want to display the configuration.

Defaults

By default, the Capitve Portal session limit and login retry count are displayed for all 802.1x ports if the *slot/port* parameter is not specified.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- Use the *slot/port* parameter to display the Captive Portal configuration for a specific 802.1x port.
- This command only displays information for 802.1x ports that are configured with a Captive Portal device classification policy.

Examples

```
-> show 802.1x captive-portal configuration

802.1x Captive Portal configuration for slot 7 port 11:

  Session Limit (hours)       = 4,
  Login Retry Count           = 5,

802.1x Captive Portal configuration for slot 8 port 1:

  Session Limit (hours)       = 8,
  Login Retry Count           = 2,

-> show 802.1x captive-portal configuration 8/1

802.1x Captive Portal configuration for slot 8 port 1:

  Session Limit (hours)       = 8,
  Login Retry Count           = 2,
```

output definitions

Session Limit (hours)	The length of the Captive Portal session, in hours.
Login Retry Count	The number of login retries allowed.

Release History

Release 6.6.1; command introduced.

Related Commands

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 802.1x ports.

MIB Objects

```
alaDot1xAuthPolicyTable
   alaDot1xCaptivePortalSessionLimit
   alaDot1xCaptivePortalRetryCnt
```

51 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 appid level
swlog remote command-log
swlog output
swlog output flash file-size
swlog clear
show log swlog
show swlog

swlog

Enables or disables switch logging. Switch logging allows you to view a history of various switch activities in a text format.

swlog

no swlog

Syntax Definitions

N/A

Defaults

By default, switch logging is enabled.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A

Examples

```
-> swlog
-> no swlog
```

Release History

Release 6.6.1; command introduced.

Related Commands

swlog appid level	Defines the level at which switch logging information is filtered for the specified application.
swlog output flash file-size	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 includes 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 to 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-auth1-2	**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 6450, 6350

Usage Guidelines

Use the ID name (**system**) or the numeric equivalent to specify the facility ID.

Examples

```
-> swlog syslog-facility-id system
-> swlog syslog-facility-id 3
-> swlog syslog-facility-id user
-> swlog syslog-facility-id 1
```

Release History

Release 6.6.3; command introduced.

Related Commands

swlog	Enables or disables switch logging.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

NA

swlog appid level

Defines the level at which switch logging information is 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***} level {***level* **|** *integer***}**

no swlog appid *app_id*

Syntax Definitions

app_id	An application identification keyword. Current application IDs are listed in the following table.
integer	A numerical equivalent value for the application ID. Current numeric equivalent values are listed in the following table.

Application IDs Supported and their Numeric Equivalents

802.1q - 7	interface - 6ip - 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	lanpower - 108	session - 71
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	web - 69
idle - 255	port-mgr - 64	

level	The severity level filter keyword value for the application ID *(see table on the following page)*. All switch logging messages of the specified level and lower 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.
integer	A numerical equivalent value for the severity level *(see table on the following page)*. All switch logging messages of the specified level and lower 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 6450, 6350

Usage Guidelines

- You can enter multiple application IDs in the command line. Separate each application ID with a space and no comma.
- Application IDs can be entered in any order.
- This command can also be used on the secondary CMM.

Note. The console messages `"+++ healthMonCpuStatus Crossed Below The Threshold Limit "` can be seen on switch bootup if it is configured to receive health monitoring debug messages on console or swlog file using the **swlog appid** and **swlog output** commands.

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 6.6.1; command introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog output flash file-size	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 6450, 6350

Usage Guidelines

N/A

Examples

```
-> swlog remote command-log enable
-> swlog remote command-log disable
```

Release History

Release 6.3.4; command was introduced.

Related Commands

swlog output flash file-size	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***]}**

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 **/flash** file system of the switch.
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.

Defaults

parameter	default
console | **flash** | **socket**	**flash** and **console**

Platforms Supported

OmniSwitch 6450, 6350

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 12) using the **socket** keyword, followed by the IP address of the remote host.

Examples

```
-> swlog output console
-> no swlog output flash
-> swlog output socket 14.1.1.1
-> swlog output socket 15.1.1.1
-> swlog output socket 16.1.1.1
-> swlog output socket 17.1.1.1
```

Release History

Release 6.6.1; command introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid level	Defines the level at which switch logging information is filtered for the specified application.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
   systemSwitchLoggingFlash
   systemSwitchLoggingSocket
   systemSwitchLoggingSocketIpAddr
   systemSwitchLoggingConsole
systemSwitchLoggingHostTable
   systemSwitchLoggingHostIpAddr
   systemSwitchLoggingHostPort
   systemSwitchLoggingHostStatus
```

swlog output flash file-size

Configures the size of the switch logging file.

swlog output flash file-size *bytes*

Syntax Definitions

bytes	The size of the switch logging file. The minimum value is 32000 while the maximum value is the total amount of free space in flash memory.

Defaults

parameter	default
bytes	128000

Platforms Supported

OmniSwitch 6450, 6350

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 6.6.1; 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 6450, 6350

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 6.6.1; command introduced.

Related Commands

swlog output flash file-size	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 time until which the switch logging information must 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	interface - 6	psm - 81
aaa - 20	ip - 15	qdispatcher - 3
amap - 18	ipc-diag - 1	qdriver - 2
bridge - 10	ip-helper - 22	qos - 13
chassis - 64	ipc-link - 4	rmon - 79
cli - 67	ipc-mon - 21	rsvp - 14
config - 66	ipms - 17	session - 71
dbggw - 89	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	web - 69
idle - 255	port-mgr - 64	

level	A numerical equivalent value for the severity level *(see the following table)*. All switch logging messages of the specified level and lower are 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 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

N/A

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- When the switch is in ASA enhanced mode, both user name and password is prompted to view the SWLOG data using **show log swlog** command. Only those users who provide the valid ASA credentials are allowed to view the data. For more information on Authenticated Switch Access - Enhanced Mode mode, refer chapter Managing Switch Security in *OmniSwitch AOS Release 6 Switch Management Guide.*
- When the switch logging display is too long, you can 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 'swlog2.log'
FILEID: fileName[swlog2.log], endPtr[32]
configSize[64000], currentSize[64000], mode[2]
Displaying file contents for 'swlog1.log'
FILEID: fileName[swlog1.log], endPtr[395]
configSize[64000], currentSize[64000], mode[1]

Time Stamp               Application Level   Log Message

-----------------------+-----------+-----+-------------------------------

MON NOV 11 12:42:11 2002     SYSTEM info   Switch Logging files cleared by
command
MON NOV 11 13:07:26 2002     WEB    info The HTTP session login successful!
MON NOV 11 13:18:24 2002     WEB    info The HTTP session login successful!
MON NOV 11 13:24:03 2002     TELNET info New telnet connection, Address ,
128.251.30.88
```

```
MON NOV 11 13:24:03 2002 TELNET    info  Session 4, Created
MON NOV 11 13:59:04 2002     WEB    info  The HTTP session user logout successful!
```

When the switch is in ASA enhanced mode, both user name and password is prompted to view the SWLOG data using **show log swlog** command.

```
-> show log swlog
Username: test
Password:   *******
```

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 6.6.1; command introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid level	Adds or removes a filter level for a specified subsystem.
swlog output flash file-size	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.

MIB Objects

N/A

show swlog

Displays switch logging information (for example, switch logging status, log devices, facility IDs with non-default severity level settings).

show swlog

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6450, 6350

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                        : console,
Syslog FacilityID                   : system(3),
Remote command-log                  : Disabled,
Console Display Level               : info (6),
All Applications Trace Level        : info (6)

All Applications have their trace level set to the level 'info' (6)
```

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 includes in the priority (PRI) section of the event message.
Console Display Level	The Console Display Level. Levels include alarm (2), error (3), alert (4), warning (5), info (6), debug1 (7), debug2 (8), and debug3 (9).
All Applications Trace 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 6.6.1; command introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid level	Defines the level at which switch logging information is filtered for the specified application.
swlog output flash file-size	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.

MIB Objects

N/A

52 OmniVista Cirrus Commands

OmniVista Cirrus is a network management solution to deliver zero touch provisioning using cloud.

OV Cirrus solution provides reduced costs, ease of devices provisioning and a unified wired/wireless management from the cloud. The solution also provides an ability to identify each device uniquely and provide a freemium/premium solution based on the user policy.

Deployment of OV Cirrus provides easy to use management and monitoring tools in a network and the ability to manage the network using devices ranging from workstations to smart phones.

MIB information for the OV Cirrus commands is as follows:

Filename: ALCATEL-IND1-CLOUD-AGENT-MIB.mib
Module: alcatelIND1SystemMIBObjects 11

A summary of the available commands is listed here.

cloud-agent admin-state
show cloud-agent status
show cloud-agent vpn status

cloud-agent admin-state

Enables or disables OV Cirrus functionality globally for the switch.

cloud-agent admin-state {enable | disable | disable force | restart}

Syntax Definitions

enable	Enables OV Cirrus for the switch.
disable	Disables OV Cirrus for the switch.
disable force	Disables OmniVista Cirrus for the switch and disconnects from the VPN.
restart	Restart option implicitly triggers "**disable force**" followed by "**enabled**".

Defaults

By default, OV Cirrus is globally enabled for the switch.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- OV Cirrus is globally enabled for the switch only when the switch boots up without a configuration file [*boot.cfg*].
- If the switch boots up with a configuration file, the feature is enabled only if OV Cirrus admin state is explicitly enabled using **cloud-agent admin-state** command.
- The switch must have access to the DHCP server in the customer network with zero configurations on the devices.
- If the OV Cirrus admin state is disabled at run-time, it will take effect only after a reboot.
- If the OV Cirrus administrative state is enabled at run-time, it will immediately trigger call-home with the activation server, if a connection was not established prior to that.
- When the OV Cirrus admin state is disabled at run-time during the connection is in progress or established, it will not have any consequences on the switch. If **write memory** is issued, the switch will not call-home even if the switch reboots or has a takeover.
- The restart option implicitly triggers the administrative states of **disable force** followed by **enable.** This will enable a user to restart call-home from OmniVista Cirrus.
- If the switch is in an intermediate state (downloading an image from image server, pre-provisioning, write memory, flash syncro, call-home, etc.), the **cloud agent admin state disable force** will display an error message: "*OV Cloud agent is in progress. Please retry after some time.*"
- When an OmniSwitch is booted without a *boot.cfg*, the device comes up without NTP wait, **show configuration snapshot ntp** says "*ERROR: System is busy. Please try later (1012) after call-home restart*". While cloud agent is restarted, there are some commands which will be applied and certain

file used by cloud agent will get updated. When the **show configuration snapshot** is attempted when these configuration/file modifications are happening, it will throw the system busy error.

Examples

```
-> cloud-agent admin-state enable
-> cloud-agent admin-state disable
-> cloud-agent admin-state disable force
-> cloud-agent admin-state restart
```

Release History

Release 6.7.2.R03; command introduced.
Release 6.7.2.R04; **restart** parameter added.

Related Commands

show cloud-agent status	Displays the Cloud Agent status and parameters received from the DHCP and activation server.
show cloud-agent vpn status	Displays the Cloud Agent VPN status.

MIB Objects

```
ovCloudAgent
   alaCloudAgntAdminState
```

show cloud-agent status

Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

show cloud-agent status

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

- The command **show cloud-agent status** will be displayed only if call home is enabled. Else, only the default values, if present, will be displayed.
- DHCP address, DHCP IP address mask, Gateway, Activation Server, Proxy Server , NTP Server will be displayed based on the DHCP response parameters received.
- DNS server, DNS domain will get displayed with the current DNS configuration in the switch, if call home is enabled. The values are displayed in this command only if the DHCP server returns these values.

Examples

```
-> show cloud-agent status
Admin State                  : Enabled,
Activation Server State      : completeOK,
Device State                 : DeviceManaged,
Error State                  : None,
Cloud Group                  : puwl71julmofjl,
DHCP Address                 : 122.1.1.27,
DHCP IP Address Mask         : 255.255.255.0,
Gateway                      : 122.1.1.254,
Activation Server            : activation.dev.myovcloud.com:443,
Network ID                   : -,
NTP Server                   : -,
DNS Server                   : 8.8.8.8,2.2.2.2,10.67.0.254,
DNS Domain                   : dns1.dc.a;le-international.com,
Proxy Server                 : 192.168.254.49:8080,
VPN Server                   : puwl71julmofjl.tenant.vpn.dev.myovcloud.com:443,
Pre-provision Server         : puwl71julmofjl.tenant.ovd.dev.myovcloud.com:80,
OV Tenant                    : omniswitch.ov.dev.ovcirrus.com:443,
VPN DPD Time (sec)           : -,
Image Server                 : -,
Image Download Retry count   : -,
Discovery Interval (min)     : 30,
Time to Next Call Home (sec) : 1550,
```

```
Call-home Timer Status       : RUNNING,
Discovery Retry Count        : 0
Certificate Status           : CONSISTENT
```

output definitions

Admin State	Refers to OV Cirrus admin status. **Enabled** or **Disabled**.
Activation Server State	Displays the status of Activation server. The various Activation Server State are: - completeOK - clientCertificateRequested - gotCertificate - failedToGetCertificate - deviceCloudManaged - clientCertificatePreviouslyIssued - upgradeSw - failedVCMixedAccounts - failedDeviceVerification - vpnConfigFailed - upgradeFailed
Device State	Displays the device status. The various device state are: - Initial - CallHomeSent - UpgradeInProgress - UpgradeInProgressRetry - VpnConnectInProgress - DeviceNotManaged - PreprovisionInProgress - PreprovisionFailed - DeviceManaged - Error
Error State	Displays the error status of the cloud agent. The various error state are: - None - CallHomeFailure - CertificateRequested - CertificateFailure - CertificatePreviouslyIssued - IncompatibleVcUnits - UpgradeDownloadFailure - UpgradeVerifyFailure - UpgradeImgFileStatusFailure - UpgradeReloadFailure - VpnConnectFailure - PreprovisionHelloOVFailure - PreprovisionCLIApplyFailure - PreprovisionConfigStatusFailure - PreprovisionWriteMemoryFailure - PreprovisionWriteCertifyStatusFailure - UnknownCloudProcessStatus - UpgradeFailed
Cloud Group	Displays the name of the group of switches of the customer.
DHCP Address	Displays the IP Address assigned by the DHCP server.

output definitions (continued)

DHCP Address IP Mask	Displays the IP Mask assigned by the DHCP server.
Gateway	Displays the IP Gateway Address assigned by the DHCP server.
Activation Server	The URL of the activation server assigned by the DHCP server.
Network ID	The DHCP VSO specific to OV Cirrus.
NTP Server	Displays all the NTP Server Address. The NTP server is displayed in IP address as well as FQDN format according to the format in which the particular server was configured.
DNS Server	Displays the DNS Server Address assigned by the DHCP server.
DNS Domain	Displays the DNS Domain Address assigned by the DHCP server.
Proxy Server	Displays the Proxy Server Address assiigned by the DHCP server.
VPN Server	The URL of the VPN server as received from the activation server.
Preprovision Server	The URL of the Preprovisioning server as received from the activation server.
OV Tenant	The URL of the OV Tenant server as received from the activation server.
VPN DPD Time (sec)	The Dead Peer Detection Time (DPD) for the VPN connection as received from the activation server.
Image Server	The URL of the image server as received from the activation server.
Image Download Retry Count	The number of attempts the switch will retry to download the image from the image server in case of failures.
Discovery Interval	The configured time in minutes after which the switch will re-attempt to connect with the activation server in case of failure/ automatic callhome trigger with TTNCH.
Time to next Call Home (sec)	The time left for the switch to attempt the connection with the activation server in case of failure/automatic callhome trigger with TTNCH.
Call Home Timer Status	The status of the call home timer. Running or Not-Running.
Discovery Retry Count	The number of times the switch has attempted to connect with the activation server after a failure/automatic callhome trigger with TTNCH.

Release History

Release 6.7.2.R03; command introduced.
Release 6.7.2.R05; Added Network ID parameter.

Related Commands

cloud-agent admin-state	Enables or disables OV Cirrus funtionality globally for the switch.
show cloud-agent vpn status	Displays the Cloud Agent VPN status.

MIB Objects

```
ovCloudAgent
   ovCloudAgentAdminState
```

```
ovCloudAgentDiscoveryInterval
ovCloudAgentDeviceState
ovCloudAgentTimeToNextCallhome
```

show cloud-agent vpn status

Displays the Cloud Agent VPN status.

show cloud-agent vpn status

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 6450, 6350

Usage Guidelines

N/A.

Examples

```
-> show cloud-agent vpn status
   VPN status                     : Connected,
   VPN Assigned IP                : 10.8.0.4,
   VPN DPD time (sec)             : 600
```

output definitions

VPN Status	Refers to OV Cirrus VPN status. The various VPN state are: - Connecting - OpenVPN's initial state - Wait - Waiting for initial response from server - Auth - Authenticating with server - Get_Config - Downloading configuration options from server - Assign_IP - Assigning IP address to virtual network interface - Add_Routes - Adding routes to system - Connected - Initialization sequence completed - Reconnecting - A restart has occurred - Retained - VPN connection retained - Exiting - A graceful exit is in progress
VPN Assigned IP	Displays the VPN server assigned IP for the VPN connection towards the OV Cirrus.
VPN DPD time (sec)	Displays the VPN Dead Peer Detection (DPD) time value in seconds.

Release History

Release 6.7.2.R03; command introduced.

Related Commands

cloud-agent admin-state	Enables or disables OV Cirrus funtionality globally for the switch.
show cloud-agent status	Displays the Cloud Agent status and parameters received from the DHCP and activation server.

MIB Objects

```
ovCloudAgent
   ovCloudAgentDeviceState
   ovCloudAgentVpnStatus
```

A Software License and Copyright Statements

This appendix contains Alcatel and third-party software vendor license and copyright statements.

Alcatel License Agreement

ALE USA, Inc. 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 ALE USA, Inc.. ALE USA, Inc. 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 ALE USA, Inc. 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. **ALE USA, Inc. Rights.** Licensee acknowledges and agrees that the Licensed Materials are the sole property of ALE USA, Inc. 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 ALE USA, Inc. 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.** ALE USA, Inc. considers the Licensed Files to contain valuable trade secrets of ALE USA, Inc., the unauthorized disclosure of which could cause irreparable harm to ALE USA, Inc. 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 ALE USA, Inc. harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation ALE USA, Inc. 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.** ALE USA, Inc. 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. ALE USA, Inc. 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 ALE USA, Inc. for either replacement or, if so elected by ALE USA, Inc., 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 ALE USA, Inc. 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.** ALE USA, Inc.'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 ALE USA, Inc. for the Licensed Materials. IN NO EVENT SHALL ALE USA, Inc. BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF ALE USA, Inc. 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 ALE USA, Inc. and Licensee, if any, ALE USA, Inc. is under no obligation to maintain or support the copies of the Licensed Files made and distributed hereunder and ALE USA, Inc. 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 ALE USA, Inc. and certifying to ALE USA, Inc. 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. ALE USA, Inc. may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by ALE USA,

Inc., Licensee agrees to return to ALE USA, Inc. 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 ALE USA, Inc.'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 ALE USA, Inc. 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 ALE USA, Inc. for a limited period of time. ALE USA, Inc. 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.

Copyright 1999-2000 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distributed verbatim copies of this document is granted.

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 ALE USA, Inc.. 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 ALE USA, Inc. certain warranties of performance, which warranties [or portion thereof] ALE USA, Inc. 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 ALE USA, Inc. and Licensee, Licensee shall immediately return the EMWEB Product and any back-up copy to ALE USA, Inc., and will certify to ALE USA, Inc. 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 ALE USA, Inc. 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

Copyright (C) by Beman Dawes, David Abrahams, 1998-2003. All rights reserved.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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

Copyright (C) 2000-2004. All rights reserved.

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.

Copyright (C) 1992-1993 Jean-loup Gailly. All rights reserved.

T. Internet Protocol Version 6

Copyright (C) 1982, 1986, 1990, 1991, 1993. The Regents of the University of California. 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, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the 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

CMM Commands

reload [primary | secondary] [with-fabric] [in [*hours*:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]
reload [primary | secondary] [with-fabric] cancel
OmniSwitch 6450, 6350

reload working {rollback-timeout minutes | no rollback-timeout} [in [*hours*:] *minutes* | at *hour*:*minute*]
OmniSwitch 6450, 6350

[configure] copy running-config working
OmniSwitch 6450, 6350

[configure] write memory
OmniSwitch 6450, 6350

[configure] copy working certified [flash-synchro]
OmniSwitch 6450, 6350

[configure] copy flash-synchro
OmniSwitch 6450, 6350

takeover
OmniSwitch 6450, 6350

show running-directory
OmniSwitch 6450, 6350

show reload [status]
OmniSwitch 6450, 6350

show microcode [working | certified | loaded]
OmniSwitch 6450, 6350

usb {enable | disable}
OmniSwitch 6450, 6350

usb auto-copy {enable | disable}
OmniSwitch 6450, 6350

usb disaster-recovery {enable | disable}
OmniSwitch 6450, 6350

mount [/uflash]
OmniSwitch 6450, 6350

umount /uflash
OmniSwitch 6450, 6350

show usb statistics
OmniSwitch 6450, 6350

image integrity-check {working | certified} *filename*
OmniSwitch 6450, 6350

Chassis Management and Monitoring Commands

system contact *text_string*
OmniSwitch 6450, 6350

system name *text_string*
OmniSwitch 6450, 6350

system location *text_string*
OmniSwitch 6450, 6350

system date [*mm/dd/yyyy*]
OmniSwitch 6450, 6350

system time [*hh:mm:ss*]
OmniSwitch 6450, 6350

system time-and-date synchro

OmniSwitch 6450, 6350

system timezone [*timezone_abbrev* | *offset_value* | *time_notation*]
OmniSwitch 6450, 6350

system daylight savings time [{enable | disable} | start {*week*} {*day*} in {*month*} at {*hh:mm*} end {*week*} {*day*} in {*month*} at {*hh:mm*} [by *min*]]
OmniSwitch 6450, 6350

update {uboot {cmm | ni {all | *slot*}} **uboot-miniboot** | fpga cmm | *bootrom {all | slot} | [default | backup] miniboot [all | slot]}*
OmniSwitch 6450, 6350

update lanpower {*lanpower_num* | *all*}
OmniSwitch 6450, 6350

reload ni [slot] *number*
OmniSwitch 6450, 6350

reload all [in [*hours*:] *minutes* | at *hour*:*minute* [*month day* | *day month*]]
reload all cancel
OmniSwitch 6450, 6350

reload pass-through *slot-number*
OmniSwitch 6450, 6350

power ni [slot] *slot-number*
no power ni [slot] *slot-number*
OmniSwitch 6450, 6350

temp-threshold *temp* slot *slot-number*
OmniSwitch 6450, 6350

stack set slot *slot-number* saved-slot *saved-slot-number* [reload]
OmniSwitch 6450, 6350

stack set slot *slot-number* mode {stackable | standalone} [reload]
stack clear slot *slot-number* [immediate]

OmniSwitch 6450, 6350

hash-control mode fdb { xor | crc }
OmniSwitch 6450, 6350

hash-control load-balance non-ucast {enable | disable}
OmniSwitch 6450, 6350

show system
OmniSwitch 6450, 6350

show hardware info
OmniSwitch 6450, 6350

show chassis [*number*]
OmniSwitch 6450, 6350

show cmm [*number*]
OmniSwitch 6450, 6350

show ni [*number*]
OmniSwitch 6450, 6350

show module [*number*]
OmniSwitch 6450, 6350

show module long [*number*]
OmniSwitch 6450, 6350

show module status [*number*]
OmniSwitch 6450, 6350

show power [supply] [*number*]
OmniSwitch 6450, 6350

show fan [*number*]
OmniSwitch 6450, 6350

show temperature [*number*]
OmniSwitch 6450, 6350

show stack topology [*slot-number*]
OmniSwitch 6450, 6350

show stack status
OmniSwitch 6450, 6350

show stack mode
OmniSwitch 6450, 6350

show hash-control [mode fdb]
OmniSwitch 6450, 6350

show system hardware-self-test
OmniSwitch 6450, 6350

show system process-self-test
OmniSwitch 6450, 6350

license apply
OmniSwitch 6450

license remove feature {metro | gig | 10G}
OmniSwitch 6450

license unlock feature {metro | gig | 10G}
OmniSwitch 6450

show license info
OmniSwitch 6450

show license file [filename | local]
OmniSwitch 6450

stack split-protection {enable | disable}
OmniSwitch 6450, 6350

[no] stack split-protection linkaggid linkagg-id
OmniSwitch 6450, 6350

stack split-protection guard-timer *time*
OmniSwitch 6450, 6350

stack split-protection helper {enable | disable}
OmniSwitch 6450, 6350

stack split-detection helper linkagg linkagg-id
OmniSwitch 6450, 6350

show stack split-protection status
OmniSwitch 6450, 6350

show stack split-protection statistics
OmniSwitch 6450, 6350

show stack split-protection stacking-units
OmniSwitch 6450, 6350

show stack split-protection helper status
OmniSwitch 6450, 6350

Chassis MAC Server (CMS) Commands

mac-range eeprom *start_mac_address count*
OmniSwitch 6450, 6350

mac-retention status {**enable | disable**}
OmniSwitch 6450, 6350

mac-retention dup-mac-trap {**enable | disable**}
OmniSwitch 6450, 6350

mac release
OmniSwitch 6450, 6350

show mac-range [*index*]

OmniSwitch 6450, 6350

show mac-range [*index*] alloc
OmniSwitch 6450, 6350

show mac-retention status
OmniSwitch 6450, 6350

Power over Ethernet (PoE) Commands

lanpower start {*slot/port*[*-port2*] | *slot*}
OmniSwitch 6450, 6350

lanpower *slot* delayed-start {enable | disable} [*value*]
OmniSwitch 6450, 6350

lanpower stop {*slot/port*[*-port2*] | *slot*}
OmniSwitch 6450, 6350

lanpower {*slot/port* | *slot*} power *milliwatts*
OmniSwitch 6450, 6350

lanpower *slot* maxpower *watts*
OmniSwitch 6450, 6350

lanpower *slot/port* priority {critical | high | low}
OmniSwitch 6450, 6350

lanpower *slot* priority-disconnect {enable | disable}
OmniSwitch 6450, 6350

lanpower *slot* combo-port {enable | disable}
N/A

lanpower *slot* high-resistance-detection {enable | disable}
OmniSwitch 6450, 6350

lanpower *slot* capacitor-detection {enable | disable}
OmniSwitch 6450, 6350

show lanpower *slot*
OmniSwitch 6450, 6350

show lanpower delayed-start *slot*
OmniSwitch 6450, 6350

show lanpower capacitor-detection *slot*
OmniSwitch 6450, 6350

show lanpower priority-disconnect *slot*
OmniSwitch 6450, 6350

show lanpower high-resistance-detection *slot*
OmniSwitch 6450, 6350

Network Time Protocol Commands

ntp server {*ip_address* | *domain_name*} [key *key* | version *version* | minpoll *exponent* | prefer | burst | iburst]
no ntp server {*ip_address* | *domain_name*}
OmniSwitch 6450, 6350

ntp server synchronized
OmniSwitch 6450, 6350

ntp server unsynchronized
OmniSwitch 6450, 6350

ntp client {enable | disable}
OmniSwitch 6450, 6350

ntp broadcast {enable | disable}
OmniSwitch 6450, 6350

ntp broadcast delay *microseconds*
OmniSwitch 6450, 6350

ntp key *key* [trusted | untrusted]
OmniSwitch 6450, 6350

ntp key load
OmniSwitch 6450, 6350

show ntp client
OmniSwitch 6450, 6350

show ntp client server-list
OmniSwitch 6450, 6350

show ntp server status [*ip_address* | *domain_name*]
OmniSwitch 6450, 6350

show ntp keys
OmniSwitch 6450, 6350

Session Management Commands

session login-attempt integer
OmniSwitch 6450, 6350

session login-timeout *seconds*
OmniSwitch 6450, 6350

session banner {cli | ftp | http} file_name
session banner no {cli | ftp | http}
OmniSwitch 6450, 6350

session timeout {cli | http | ftp} *minutes*
OmniSwitch 6450, 6350

session prompt default {<num> | <string> | system-name}
OmniSwitch 6450, 6350

session console {enable | disable}
OmniSwitch 6450, 6350

session xon-xoff {**enable** | **disable**}
OmniSwitch 6450, 6350

session cli-auto-complete-space {**enable** | **disable**}
OmniSwitch 6450, 6350

prompt [user] [time] [date] [string *string*] [prefix]
no prompt
OmniSwitch 6450, 6350

show prefix
OmniSwitch 6450, 6350

alias *alias command_name*
OmniSwitch 6450, 6350

show alias
OmniSwitch 6450, 6350

user profile save
OmniSwitch 6450, 6350

user profile save global-profile
OmniSwitch 6450, 6350

user profile reset
OmniSwitch 6450, 6350

history size *number*
OmniSwitch 6450, 6350

show history [parameters]
OmniSwitch 6450, 6350

!{! | *n*}
OmniSwitch 6450, 6350

command-log {enable | disable}
OmniSwitch 6450, 6350

kill *session_number*

OmniSwitch 6450, 6350

exit
OmniSwitch 6450, 6350

whoami
OmniSwitch 6450, 6350

who
OmniSwitch 6450, 6350

show session config
OmniSwitch 6450, 6350

show session xon-xoff
OmniSwitch 6450, 6350

more size *lines*
OmniSwitch 6450, 6350

more
no more
OmniSwitch 6450, 6350

show more
OmniSwitch 6450, 6350

telnet {*host_name* | *ip_address***}**
OmniSwitch 6450, 6350

telnet6 {*ipv6_address* | *hostname***} [***if_name***]**
OmniSwitch 6450, 6350

ssh {tcp-port port-number | *host_name* | *ip_address* | **enable** | **disable}**
OmniSwitch 6450, 6350

ssh6 {*ipv6_address* | *hostname***} [***if_name***]**
OmniSwitch 6450, 6350

ssh enforce pubkey-auth {enable | disable}
OmniSwitch 6450, 6350

show ssh config
OmniSwitch 6450, 6350

show command-log
OmniSwitch 6450, 6350

show command-log status
OmniSwitch 6450, 6350

File Management Commands

cd [*path*]
OmniSwitch 6450, 6350

pwd
OmniSwitch 6450, 6350

mkdir [*path/*]*dir*
OmniSwitch 6450, 6350

rmdir [*path/*]*dir*
OmniSwitch 6450, 6350

ls [-r] [[*path/*]*dir*]
OmniSwitch 6450, 6350

dir [[*path/*]*dir*]
OmniSwitch 6450, 6350

rename [*path/*]*old_name* [*path/*]*new_name*
OmniSwitch 6450, 6350

rm [-r] [*path/*]*filename*
OmniSwitch 6450, 6350

delete [*path/*]*filename*
OmniSwitch 6450, 6350

cp [-r] [*path/*]*orig_filename* [*dest_path/*]*dupl_filename*
OmniSwitch 6450, 6350

scp *user_name@remote_ip_addr:[path/]source [path/]target*
scp *[path/]source user_name@remote_ip_addr:[path/]target*
OmniSwitch 6450, 6350

mv {[*path/*]*filename dest_path*[*/new_filename*] | [*path/*]*dir dest_path*[*/new_dir*]}
OmniSwitch 6450, 6350

move {[*path/*]*filename dest_path*[*/new_filename*] | [*path/*]*dir dest_path*[*/new_dir*]}
OmniSwitch 6450, 6350

chmod {+w | -w} [*path/*]*file*
OmniSwitch 6450, 6350

attrib {+w | -w} [*path/*]*file*
OmniSwitch 6450, 6350

freespace [**/flash**]
OmniSwitch 6450, 6350

fsck **/flash [no-repair | repair]**
OmniSwitch 6450, 6350

newfs **/flash**
OmniSwitch 6450, 6350

rcp [slot:**]** source_filepath **[**slot:**]** destination_filepath
OmniSwitch 6450, 6350

rrm *slot filepath*
OmniSwitch 6450, 6350

rls *slot directory* [*file_name*]
OmniSwitch 6450, 6350

vi [*path/*]*filename*
OmniSwitch 6450, 6350

view [*path/*]*filename*
OmniSwitch 6450, 6350

tty *lines columns*
OmniSwitch 6450, 6350

show tty
OmniSwitch 6450, 6350

more [*path/*]*file*
OmniSwitch 6450, 6350

ftp {*host_name* | *ip_address***}**
OmniSwitch 6450, 6350

OmniSwitch 6450, 6350

scp-sftp {**enable** | **disable}**
OmniSwitch 6450, 6350

show ssh config
OmniSwitch 6450, 6350

sftp {*host_name* | *ip_address***}**
OmniSwitch 6450, 6350

sftp6 {*host_name* | *ipv6_address***} [***if_name***]**
OmniSwitch 6450, 6350

tftp {*host_name* | *ip_address*} **{get** | **put} source-file [src_path/]***src_file*
[destination-file [dest_path/] *dest_file***] [ascii]**
OmniSwitch 6450, 6350

rz
OmniSwitch 6450, 6350

Web Management Commands

{[ip] http | https} server
no {[ip] http | https} server
OmniSwitch 6450, 6350

{[ip] http | https} ssl
no {[ip] http | https} ssl
OmniSwitch 6450, 6350

[ip] http port {default | *port*}
OmniSwitch 6450, 6350

https port {default | *port*}
OmniSwitch 6450, 6350

debug http sessiondb
OmniSwitch 6450, 6350

show [ip] http
OmniSwitch 6450, 6350

webview wlan cluster-virtual-ip *virtual-ip-address-of-wlan-cluster*
OmniSwitch 6450, 6350

webview wlan cluster-virtual-ip precedence {lldp | configured}
OmniSwitch 6450, 6350

show webview wlan config
OmniSwitch 6450, 6350

Configuration File Manager Commands

configuration apply *filename* [at *hh:mm month dd* [*year*]] | [in *hh*[*:mm*]] [verbose]
OmniSwitch 6450, 6350

configuration error-file limit *number*
OmniSwitch 6450, 6350

show configuration status
OmniSwitch 6450, 6350

configuration cancel
OmniSwitch 6450, 6350

configuration syntax check *path/filename* [verbose]
OmniSwitch 6450, 6350

configuration snapshot *feature_list* [*path/filename*]
OmniSwitch 6450, 6350

show configuration snapshot [*feature_list*]
OmniSwitch 6450, 6350

write terminal
OmniSwitch 6450, 6350

SNMP and OpenFlow Commands

snmp station {*ip_address* | *ipv6_address*} {[*udp_port*] [*username*] [v1 | v2 | v3] [enable | disable]}
no snmp station {*ip_address* | *ipv6_address*}
OmniSwitch 6450, 6350

snmp soure ip preferred {default | no-loopback | *ip_address*}
no snmp source ip preferred
OmniSwitch 6450, 6350

show snmp station
OmniSwitch 6450, 6350

snmp community map *community_string* {[user *useraccount_name*] | {enable | disable}}
no snmp community map *community_string*
OmniSwitch 6450, 6350

snmp community map mode {enable | disable}
OmniSwitch 6450, 6350

show snmp community map
OmniSwitch 6450, 6350

snmp security {no security | authentication set | authentication all | privacy set | privacy all | trap only}
OmniSwitch 6450, 6350

show snmp security
OmniSwitch 6450, 6350

show snmp statistics
OmniSwitch 6450, 6350

show snmp mib family [*table_name*]
OmniSwitch 6450, 6350

snmp trap absorption {enable | disable}
OmniSwitch 6450, 6350

snmp trap to webview {enable | disable}
OmniSwitch 6450, 6350

snmp trap replay {*ip_address* | *ipv6_address***}** [*seq_id*]
OmniSwitch 6450, 6350

snmp trap filter {*ip_address* | *ipv6_address*} *trap_id_list*
no snmp trap filter {*ip_address* | *ipv6_address***}** *trap_id_list*
OmniSwitch 6450, 6350

snmp authentication trap {enable | disable}
OmniSwitch 6450, 6350

show snmp trap replay
OmniSwitch 6450, 6350

show snmp trap filter
OmniSwitch 6450, 6350

show snmp authentication trap
OmniSwitch 6450, 6350

show snmp trap config
OmniSwitch 6450, 6350

snmp view *viewname* oid-tree {include | exclude}
no snmp view *viewname* oid-tree
OmniSwitch 6450, 6350

show snmp views
OmniSwitch 6450, 6350

show snmp view *viewname*
OmniSwitch 6450, 6350

openflow back-off-max *seconds*
OmniSwitch 6450

openflow idle-probe-timeout *seconds*
OmniSwitch 6450

openflow logical-switch name [admin-state {enable | disable}] [mode {normal | api}] [version {1.0 | 1.3.1}+] [vlan *vlan_id*]
no openflow logical-switch <name>
OmniSwitch 6450

openflow logical-switch name controller ip_address [:port] admin-state {enable | disable}
no openflow logical-switch name controller ip_address [:port]
OmniSwitch 6450

openflow logical-switch name interfaces {port slot/port1[-port2] | linkagg agg_id[-*agg_id2*]}

no openflow logical-switch name interfaces {port slot/port1[-port2] | linkagg agg_id[-*agg_id2*]}
OmniSwitch 6450

show openflow
OmniSwitch 6450

show openflow logical-switch [name | controllers | interfaces]
OmniSwitch 6450

show openflow logical-switch name {flowtable | flowentry | openflowport | group} stats
OmniSwitch 6450

DNS Commands

ip domain-lookup
no ip domain-lookup
OmniSwitch 6450, 6350

ip name-server *server-address1* [*server-address2* [*server-address3*]]
OmniSwitch 6450, 6350

ipv6 name-server *server-ipv6_address1* [*server-ipv6_address2* [*server-ipv6_address3*]]
OmniSwitch 6450, 6350

ip domain-name *name*
no ip domain-name
OmniSwitch 6450, 6350

show dns
OmniSwitch 6450, 6350

Link Aggregation Commands

static linkagg *agg_num* size *size* [name *name*] [admin state {enable | disable}]
no static linkagg *agg_num*
OmniSwitch 6450, 6350

static linkagg *agg_num* name *name*
static linkagg *agg_num* no name
OmniSwitch 6450, 6350

static linkagg *agg_num* admin state {enable | disable}
OmniSwitch 6450, 6350

static agg [ethernet | fastethernet | gigaethernet] *slot*/*port* agg num *agg_num*
static agg no [ethernet | fastethernet | gigaethernet] *slot*/*port*
OmniSwitch 6450, 6350

lacp linkagg *agg_num* size *size*
no lacp linkagg *agg_num*
OmniSwitch 6450, 6350

lacp linkagg *agg_num* name *name*
lacp linkagg *agg_num* no name
OmniSwitch 6450, 6350

lacp linkagg *agg_num* admin state {enable | disable}
OmniSwitch 6450, 6350

lacp linkagg *agg_num* actor admin key *actor_admin_key*
lacp linkagg *agg_num* no actor admin key
OmniSwitch 6450, 6350

lacp linkagg *agg_num* actor system priority *actor_system_priority*
lacp linkagg *agg_num* no actor system priority
OmniSwitch 6450, 6350

lacp linkagg *agg_num* actor system id *actor_system_id*
lacp linkagg *agg_num* no actor system id
OmniSwitch 6450, 6350

lacp linkagg *agg_num* partner system id *partner_system_id*
lacp linkagg *agg_num* no partner system id
OmniSwitch 6450, 6350

lacp linkagg *agg_num* partner system priority *partner_system_priority*
lacp linkagg *agg_num* no partner system priority
OmniSwitch 6450, 6350

lacp linkagg *agg_num* partner admin key *partner_admin_key*
lacp linkagg *agg_num* no partner admin key
OmniSwitch 6450, 6350

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor admin key *actor_admin_key*
lacp agg no [ethernet | fastethernet | gigaethernet] *slot*/*port*
OmniSwitch 6450, 6350

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}
OmniSwitch 6450, 6350

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor system id *actor_system_id*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no actor system id
OmniSwitch 6450, 6350

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor system priority *actor_system_priority*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no actor system priority
OmniSwitch 6450, 6350

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}
OmniSwitch 6450, 6350

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
OmniSwitch 6450, 6350

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin key *partner_admin_key*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no partner admin key
OmniSwitch 6450, 6350

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
OmniSwitch 6450, 6350

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* actor port priority *actor_port_priority*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no actor port priority
OmniSwitch 6450, 6350

lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* partner admin port *partner_admin_port*
lacp agg [ethernet | fastethernet | gigaethernet] *slot*/*port* no partner admin port
OmniSwitch 6450, 6350

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
OmniSwitch 6450, 6350

show linkagg [*agg_num*]
OmniSwitch 6450, 6350

show linkagg [agg_num] port [*slot*/*port*]
OmniSwitch 6450, 6350

show linkagg agg_num [-*agg_num2*] accounting
OmniSwitch 6450, 6350

show linkagg agg_num [-*agg_num2*] counters [errors]
OmniSwitch 6450, 6350

show linkagg agg_num [-*agg_num2*] traffic
OmniSwitch 6450, 6350

linkagg {all | agg_num [-*agg_num2*]} no l2-statistics
OmniSwitch 6450, 6350

dhl num *dhl_num [name name]*
no dhl num *dhl_num*
OmniSwitch 6450, 6350

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}
OmniSwitch 6450, 6350

dhl num *dhl_num admin-state* {enable | disable}
OmniSwitch 6450, 6350

dhl num *dhl_num vlan-map linkb {vlan_id [-vlan_id]}*
no dhl num *dhl_num vlan-map linkb {vlan_id [-vlan_id]}*
OmniSwitch 6450, 6350

dhl num *dhl_num pre-emption-time num*
OmniSwitch 6450, 6350

dhl num *dhl_num mac-flushing* {none | raw | mvrp}
OmniSwitch 6450, 6350

show dhl
OmniSwitch 6450, 6350

show dhl num *dhl_num*
OmniSwitch 6450, 6350

show dhl num *dhl_num* [linkA | linkB]
OmniSwitch 6450, 6350

802.1AB Commands

lldp destination mac-address {nearest-bridge | nearest-edge}
OmniSwitch 6450, 6350

lldp transmit fast-start-count num
OmniSwitch 6450, 6350

lldp transmit interval seconds
OmniSwitch 6450, 6350

lldp transmit hold-multiplier num
OmniSwitch 6450, 6350

lldp transmit delay seconds
OmniSwitch 6450, 6350

lldp reinit delay seconds
OmniSwitch 6450, 6350

lldp notification interval seconds
OmniSwitch 6450, 6350

lldp {slot/port | slot | chassis} lldpdu {tx | rx | tx-and-rx | disable}
OmniSwitch 6450, 6350

lldp {slot/port | slot | chassis} notification {enable | disable}

OmniSwitch 6450, 6350

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]
OmniSwitch 6450, 6350

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]
OmniSwitch 6450, 6350

lldp {slot/port | slot | chassis} tlv management {port-description | system-name | system-description | system-capabilities | management-address} {enable | disable}
OmniSwitch 6450, 6350

lldp {slot/port | slot | chassis} tlv dot1 {port-vlan | vlan-name} {enable | disable}
OmniSwitch 6450, 6350

lldp {slot/port | slot | chassis} tlv dot3 mac-phy {enable | disable}
OmniSwitch 6450, 6350

lldp {slot/port | slot | chassis} tlv dot3 power-via-mdi {enable | disable}
OmniSwitch 6450, 6350

lldp {slot/port | slot | chassis} tlv med {power | capability | network policy} {enable | disable}
OmniSwitch 6450, 6350

lldp {slot/port | slot | chassis} tlv proprietary {enable | disable}
OmniSwitch 6450, 6350

show lldp {slot | slot/port} config
OmniSwitch 6450, 6350

show lldp network-policy [policy_id]
OmniSwitch 6450, 6350

show lldp [slot | slot/port] med network-policy
OmniSwitch 6450, 6350

show lldp system-statistics
OmniSwitch 6450, 6350

show lldp [slot|slot/port] statistics
OmniSwitch 6450, 6350

show lldp local-system
OmniSwitch 6450, 6350

show lldp [slot/port | slot] local-port
OmniSwitch 6450, 6350

show lldp local-management-address
OmniSwitch 6450, 6350

show lldp [slot/port | slot] remote-system
OmniSwitch 6450, 6350

show lldp [slot/port | slot] remote-system [med {network-policy | inventory}]
OmniSwitch 6450, 6350

lldp {slot/port| slot | **chassis**} **trust-agent** {**enable** | **disable**}
lldp {slot/port| slot | **chassis**} [**chassis-id-subtype** {**chassis-component** | **interface-alias** | **port-component** | **mac-address** | **network-address** | **interface-name** | **locally-assigned** | any}]
OmniSwitch 6450, 6350

lldp {slot/port| slot | **chassis**} trust-agent violation-action {trap-and-shutdown | trap | shutdown}
OmniSwitch 6450, 6350

show lldp [num | slot/port] trusted remote-agent
OmniSwitch 6450, 6350

show lldp [num | slot/port] trust-agent
OmniSwitch 6450, 6350

Interswitch Protocol Commands

amap {enable | disable}
OmniSwitch 6450, 6350

amap discovery [time] *seconds*
OmniSwitch 6450, 6350

amap common [time] *seconds*
OmniSwitch 6450, 6350

show amap
OmniSwitch 6450, 6350

802.1Q Commands

vlan *vid* 802.1q {slot/port | aggregate_id} [*description*]
vlan *vid* no 802.1q {slot/port | aggregate_id}
OmniSwitch 6450, 6350

vlan 802.1q *slot/port* frame type {all | tagged}
OmniSwitch 6450, 6350

show 802.1q {slot/port | aggregate_id}
OmniSwitch 6450, 6350

Distributed Spanning Tree Commands

bridge mode {flat | 1x1}
OmniSwitch 6450, 6350

bridge [*instance*] protocol {stp | rstp | mstp}
OmniSwitch 6450, 6350

bridge cist protocol {stp | rstp | mstp}
OmniSwitch 6450, 6350

bridge 1x1 *vid* protocol {stp | rstp}
OmniSwitch 6450, 6350

bridge mst region name *name*
bridge mst region no name
OmniSwitch 6450, 6350

bridge mst region revision level *rev_level*
OmniSwitch 6450, 6350

bridge mst region max hops *max_hops*
OmniSwitch 6450, 6350

bridge msti *msti_id* [name *name*]
bridge no msti *msti_id*
bridge msti *msti_id* no name
OmniSwitch 6450, 6350

bridge msti *msti_id* vlan *vid_range*
bridge msti *msti_id* no vlan *vid_range*
OmniSwitch 6450, 6350

bridge [*instance*] priority *priority*
OmniSwitch 6450, 6350

bridge cist priority *priority*
OmniSwitch 6450, 6350

bridge msti *msti_id* priority *priority*
OmniSwitch 6450, 6350

bridge 1x1 *vid* priority *priority*
OmniSwitch 6450, 6350

bridge [*instance*] hello time *seconds*
OmniSwitch 6450, 6350

bridge cist hello time *seconds*
OmniSwitch 6450, 6350

bridge 1x1 *vid* hello time *seconds*
OmniSwitch 6450, 6350

bridge [*instance*] max age *seconds*
OmniSwitch 6450, 6350

bridge cist max age *seconds*
OmniSwitch 6450, 6350

bridge 1x1 *vid* max age *seconds*
OmniSwitch 6450, 6350

bridge [*instance*] forward delay *seconds*
OmniSwitch 6450, 6350

bridge cist forward delay *seconds*
OmniSwitch 6450, 6350

bridge 1x1 *vid* forward delay *seconds*
OmniSwitch 6450, 6350

bridge [*instance***]** bpdu-switching {enable | disable}
OmniSwitch 6450, 6350

bridge path cost mode {auto | 32bit}
OmniSwitch 6450, 6350

bridge [msti *msti_id*] auto-vlan-containment {enable | disable}
OmniSwitch 6450, 6350

bridge *instance* {*slot/port* | *logical_port*} {enable | disable}
OmniSwitch 6450, 6350

bridge cist {*slot/port* | *logical_port*} {enable | disable}
OmniSwitch 6450, 6350

bridge 1x1 *vid* {*slot/port* | *logical_port*} {enable | disable}
OmniSwitch 6450, 6350

bridge *instance* {*slot/port* | *logical_port*} priority *priority*
OmniSwitch 6450, 6350

bridge **cist** {*slot/port* | *logical_port*} priority *priority*
OmniSwitch 6450, 6350

bridge **msti** *msti_id* {*slot/port* | *logical_port*} priority *priority*
OmniSwitch 6450, 6350

bridge **1x1** *vid* {*slot/port* | *logical_port*} priority *priority*
OmniSwitch 6450, 6350

bridge *instance* {*slot/port* | *logical_port*} path cost *path_cost*
OmniSwitch 6450, 6350

bridge **cist** {*slot/port* | *logical_port*} path cost *path_cost*
OmniSwitch 6450, 6350

bridge **mist** *msti_id* {*slot/port* | *logical_port*} path cost *path_cost*
OmniSwitch 6450, 6350

bridge **1x1** *vid* {*slot/port* | *logical_port*} path cost *path_cost*
OmniSwitch 6450, 6350

bridge *instance* {*slot/port* | *logical_port*} mode {forwarding | blocking | dynamic}
OmniSwitch 6450, 6350

bridge cist {*slot/port* | *logical_port*} mode {dynamic | blocking | forwarding}

OmniSwitch 6450, 6350

bridge 1x1 *vid* {*slot/port* | *logical_port*} mode {dynamic | blocking | forwarding}
OmniSwitch 6450, 6350

bridge *instance* {*slot/port* | *logical_port*} connection {noptp | ptp | autoptp | edgeport}
OmniSwitch 6450, 6350

bridge cist {*slot/port* | *logical_port*} connection {noptp | ptp | autoptp | edgeport}
OmniSwitch 6450, 6350

bridge 1x1 *vid* {*slot/port* | *logical_port*} connection {noptp | ptp | autoptp | edgeport}
OmniSwitch 6450, 6350

bridge cist {*slot/port* | *logical_port*} admin-edge {on | off | enable | disable}
OmniSwitch 6450, 6350

bridge 1x1 *vid* {*slot/port* | *logical_port*} admin-edge {on | off | enable | disable}
OmniSwitch 6450, 6350

bridge cist {*slot/port* | *logical_port*} auto-edge {on | off | enable | disable}
OmniSwitch 6450, 6350

bridge 1x1 *vid* {*slot/port* | *logical_port*} auto-edge {on | off | enable | disable}
OmniSwitch 6450, 6350

bridge cist {*slot/port* | *logical_port*} {restricted-role | root-guard} {on | off | enable | disable}
OmniSwitch 6450, 6350

bridge 1x1 *vid* {*slot/port* | *logical_port*} {restricted-role | root-guard} {on | off | enable | disable}
OmniSwitch 6450, 6350

bridge cist {*slot/port* | *logical_port*} restricted-tcn {on | off | enable | disable}
OmniSwitch 6450, 6350

bridge 1x1 *vid* {*slot/port* | *logical_port*} restricted-tcn {on | off | enable | disable}
OmniSwitch 6450, 6350

bridge cist txholdcount *value*
OmniSwitch 6450, 6350

bridge 1x1 *vid* txholdcount {*value*}
OmniSwitch 6450, 6350

bridge rrstp
no bridge rrstp
OmniSwitch 6450, 6350

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*]
OmniSwitch 6450, 6350

bridge rrstp ring *ring_id* **vlan-tag vid**
OmniSwitch 6450, 6350

bridge rrstp ring *ring_id* **status {enable | disable}**
OmniSwitch 6450, 6350

show spantree [*instance*]
OmniSwitch 6450, 6350

show spantree mode
OmniSwitch 6450, 6350

show spantree cist
OmniSwitch 6450, 6350

show spantree msti [*msti_id*]

OmniSwitch 6450, 6350

show spantree 1x1 [*vid*]
OmniSwitch 6450, 6350

show spantree [*instance*] ports [forwarding | blocking | active | configured]
OmniSwitch 6450, 6350

show spantree cist ports [forwarding | blocking | active | configured]
OmniSwitch 6450, 6350

show spantree msti [*msti_id*] ports [forwarding | blocking | active | configured]
OmniSwitch 6450, 6350

show spantree 1x1 [*vid*] ports [forwarding | blocking | active | configured]
OmniSwitch 6450, 6350

show spantree mst region
OmniSwitch 6450, 6350

show spantree mst [*msti_id*] vlan-map
OmniSwitch 6450, 6350

show spantree cist vlan-map
OmniSwitch 6450, 6350

show spantree mst *vid* vlan-map
OmniSwitch 6450, 6350

show spantree mst port {*slot/port* | *logical_port*}
OmniSwitch 6450, 6350

show bridge rrstp configuration
OmniSwitch 6450, 6350

show bridge rrstp ring [*ring_id*]
OmniSwitch 6450, 6350

bridge mode 1x1 pvst+ {enable | disable}
OmniSwitch 6450, 6350

bridge port {*slot/port* | *agg_num*} pvst+ {auto | enable | disable}
OmniSwitch 6450, 6350

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
OmniSwitch 6450

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* protected-vlan *vlan_id1*[-*vlan_id2*] [*vlan_id1*[-*vlan_id2*]]
no erp-ring *ring_id* protected-vlan [*vlan_id1*[-*vlan_id2*]]
OmniSwitch 6450

erp-ring ring_id rpl-node {port *slot/port* | linkagg agg_num}
no erp-ring ring_id rpl-node
OmniSwitch 6450

erp-ring ring_id wait-to-restore wtr_timer
no erp-ring ring_id wait-to-restore
OmniSwitch 6450

erp-ring ring_id {enable | disable}
OmniSwitch 6450

erp-ring ring_id ethoam-event {port *slot/port* | linkagg agg_num} remote-endpoint mep_id
no erp-ring ring_id ethoam-event {port *slot/port* | linkagg agg_num}
OmniSwitch 6450

erp-ring ring_id guard-timer guard_timer
no erp-ring ring_id guard-timer
OmniSwitch 6450

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]**
erp-ring ring_id reset-version-fallback
erp-ring ring_id clear
clear erp statistics [ring ring_id [port *slot/port* | linkagg agg_num]]
OmniSwitch 6450

show erp [ring ring_id | [port *slot/port* | linkagg agg_num]]
OmniSwitch 6450

show erp [ring ring_id] protected-vlan
OmniSwitch 6450

show erp statistics [ring ring_id [port *slot/port* | linkagg agg_num]]
OmniSwitch 6450

Loopback Detection Commands

loopback-detection {enable | disable}
OmniSwitch 6450, 6350

loopback-detection port slot/port [-port2] {enable | disable}
OmniSwitch 6450, 6350

loopback-detection transmission-timer seconds
OmniSwitch 6450, 6350

loopback-detection autorecovery-timer seconds
show loopback-detection
OmniSwitch 6450, 6350

show loopback-detection port [slot/port]
OmniSwitch 6450, 6350

show loopback-detection statistics port [slot/port]
OmniSwitch 6450, 6350

CPE Test Head Commands

test-oam *string* [descr *description*]
no test-oam *string*
OmniSwitch 6450

test-oam *string* [direction {unidirectional | bidirectional}]
OmniSwitch 6450

test-oam string [src-endpoint src-string] [dst-endpoint dst-string]
OmniSwitch 6450

test-oam string port slot/port
OmniSwitch 6450

test-oam string [vlan svlan] [[test-frame [src-mac src-address] [dst-mac dst-address]]
OmniSwitch 6450

test-oam string role {generator | analyzer | loopback}
OmniSwitch 6450

test-oam string [duration secs] [rate rate] [packet-size bytes]
OmniSwitch 6450

test-oam string frame
OmniSwitch 6450

test-oam string l2-saa [priority vlan-priority] [count num-pkts] [interval inter-pkt-delay] [continuous] [size size] [drop-eligible {true | false}]
no test-oam string l2-saa
OmniSwitch 6450

test-oam string {[vlan vlan-id] [port slot/port] [packet-size bytes] start | stop} [fetch-remote-stats]
OmniSwitch 6450

test-oam string remote-sys-mac string
OmniSwitch 6450

test-oam statistics flash-logging {enable | disable}
OmniSwitch 6450

show test-oam [**tests** | string**]**
OmniSwitch 6450

show test-oam [string**]** statistics
OmniSwitch 6450

show test-oam [string**]** **saa** statistics
OmniSwitch 6450

clear test-oam [string] statistics
OmniSwitch 6450

test-oam *group* string [descr *description*]
no test-oam group *string*
OmniSwitch 6450

test-oam *group* string [tests string1.....string8]
test-oam group string [no tests string1.....string8]
OmniSwitch 6450

test-oam *feeder-port* slot/port
no test-oam feeder-port
OmniSwitch 6450

test-oam group string [src-endpoint src-string dst-endpoint dst-string] [src-endpoint src-string] [dst-endpoint dst-string]
OmniSwitch 6450

test-oam group name role {generator | analyzer | loopback}
OmniSwitch 6450

test-oam group string port slot/port
OmniSwitch 6450

test-oam group string [direction {unidirectional | bidirectional}]
OmniSwitch 6450

test-oam group string [duration secs] [rate rate]
OmniSwitch 6450

test-oam group string {[port slot/port] start | stop} [fetch-remote-stats]
OmniSwitch 6450

test-oam group string remote-sys-mac string
OmniSwitch 6450

clear test-oam group string statistics
OmniSwitch 6450

show test-oam group [**tests | string]**
OmniSwitch 6450

show test-oam group [string**]** **saa** statistics
OmniSwitch 6450

show test-oam group [string**]** statistics
OmniSwitch 6450

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*]
OmniSwitch 6450, 6350

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*]
OmniSwitch 6450, 6350

mac-address-table aging-time *seconds*
no mac-address-table aging-time
OmniSwitch 6450, 6350

source-learning {port *slot/port1***[**-*port2***]** | **linkagg** *linkagg_num***} {enable | disable}**
OmniSwitch 6450

hash-control chain-length default
hash-control chain-length extend
OmniSwitch 6450, 6350

show hash-control chain-length
OmniSwitch 6450, 6350

show mac-address-table [permanent | learned] [*mac_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid* | *vid1-vid2*]
OmniSwitch 6450, 6350

show mac-address-table static-multicast [*multicast_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid* | *vid1-vid2*]
OmniSwitch 6450, 6350

show mac-address-table count [*mac_address*] [slot *slot* | *slot/port*] [linkagg *link_agg*] [*vid* | *vid1-vid2*]
OmniSwitch 6450, 6350

show mac-address-table aging-time
OmniSwitch 6450, 6350

show source-learning [port *slot/port***[**-*port2***]** | linkagg *linkagg_num***]**
OmniSwitch 6450

PPPoE Intermediate Agent

pppoe-ia {enable | disable}
OmniSwitch 6450

pppoe-ia {port *slot*/*port*[-*port2*] | linkagg agg_num} {enable | disable}
OmniSwitch 6450

pppoe-ia {port *slot*/*port*[-*port2*] | linkagg agg_num} {trust | client}
OmniSwitch 6450

pppoe-ia access-node-id {base-mac | system-name | mgnt-address | user-string string}
OmniSwitch 6450

pppoe-ia circuit-id {default [atm] ascii [base-mac | system-name | interface | vlan | cvlan | interface-alias | user-string string | delimiter char]}
OmniSwitch 6450

pppoe-ia remote-id {base-mac | system-name | mgnt-address | user-string string}
OmniSwitch 6450

clear pppoe-ia statistics [port {*slot*/*port*[-*port2*] | linkagg agg_num]
OmniSwitch 6450

show pppoe-ia configuration
OmniSwitch 6450

show pppoe-ia {port {*slot*/*port*[-*port2*] | linkagg agg_num} [enabled | disabled | trusted | client]
OmniSwitch 6450

show pppoe-ia {port {*slot*/*port*[-*port2*] | linkagg agg_num} statistics
OmniSwitch 6450

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*]
OmniSwitch 6450, 6350

port-security shutdown *num* **[no-aging {enable | disable}] [convert-to-static {enable | disable}]**
[boot-up {enable | disable}] [mac-move {enable | disable}] [learn-as-static {enable | disable}]
port-security shutdown 0 default
OmniSwitch 6450, 6350

port-security *slot/port*[*-port2*] maximum *num learn-trap-threshold num*
OmniSwitch 6450, 6350

port-security *slot/port*[*-port2*] max-filtering *num*
OmniSwitch 6450, 6350

port-security {*slot/port*[*-port2*] | chassis} convert-to-static
OmniSwitch 6450, 6350

port-security *slot/port* mac *mac_address* [vlan *vlan_id*]
port-security *slot/port* no mac **{**all | *mac_address***}** [vlan *vlan_id*]
OmniSwitch 6450, 6350

port-security *slot/port*[*-port2*] mac-range [low *mac_address* | high *mac_address*]
no port security *slot/port*[*-port2*] mac-range [low *mac_address* | high *mac_address*]
OmniSwitch 6450, 6350

port-security *slot/port*[*-port2*] violation {shutdown | restrict | discard}
OmniSwitch 6450, 6350

port-security *slot/port[-port2]* release
OmniSwitch 6450, 6350

port-security *slot/port*[*-port2*] learn-trap-threshold *num*
OmniSwitch 6450, 6350

show port-security [*slot/port1-port2* | *slot/port*] [mac-range]
OmniSwitch 6450, 6350

show port-security shutdown
OmniSwitch 6450, 6350

show port-security brief
OmniSwitch 6450, 6350

Ethernet Port Commands

trap *slot*[/*port*[*-port2*]] port link {enable | disable | on | off}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[*-port2*]] speed {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[*-port2*]] autoneg {enable | disable | on | off}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[*-port2*]] crossover {auto | mdix | mdi}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[*-port2*]] pause {rx | tx-and-rx | disable}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[*-port2*]] duplex {full | half | auto}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[*-port2*]] admin {up | down}
OmniSwitch 6450, 6350

interfaces *slot*/*port* alias *description*
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[-*port2*]] ifg *bytes*
OmniSwitch 6450, 6350

[stacking] interfaces *slot* [/*port*[-*port2*]] no l2 statistics
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[-*port2*]] max frame *bytes*
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[-*port2*]] flood {broadcast | multicast | unknown-unicast | all} {enable | disable}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[-*port2*]] flood {broadcast | multicast | unknownunicast | all} rate {mbps *num* | pps *num* | percentage *num* | default}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[-*port2*]] clear-violation-all
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[-*port2*]] hybrid {fiber | copper} autoneg {enable | disable | on | off}
OmniSwitch 6450, 6350

interfaces *slot* [/*port*[-*port2*]] hybrid copper crossover {auto | mdix | mdi}
OmniSwitch 6450, 6350

interfaces *slot*[/*port*[-*port2*]] hybrid {fiber | copper} duplex {full | half | auto}
OmniSwitch 6450, 6350

interfaces *slot*[/*port*[-*port2*]] speed hybrid {fiber | copper} {auto | 10 | 100 | 1000 | 10000 | max {100 | 1000}}
OmniSwitch 6450, 6350

interfaces *slot*[/*port*[-*port2*]] hybrid {fiber | copper} pause {rx | tx-and-rx | disable}
OmniSwitch 6450, 6350

interfaces *slot*/*port* tdr-test-start
OmniSwitch 6450

interfaces [slot | *slot*/*port[-port2]]* no tdr-statistics
OmniSwitch 6450

interfaces [slot | *slot*/*port]* tdr-extended-test-start
interfaces [slot | *slot*/*port[-port2]]* no tdr-extended-statistics
interfaces transceiver ddm [trap] {enable | disable}
OmniSwitch 6450, 6350

interfaces *slot*[/*port*[-*port2*]] eee {enable | disable}
interfaces ptp {enable | disable}
show [stacking] interfaces [*slot*[/*port*[-*port2*]]]
OmniSwitch 6450, 6350

show interfaces [slot | *slot*/*port[-port2]]* tdr-statistics
OmniSwitch 6450

show interfaces [slot | *slot*/*port[-port2]]* tdr-extended-statistics
OmniSwitch 6450

show interfaces [*slot*[/*port*[-*port2*]]] capability
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] flow [control]
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] pause
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] accounting
OmniSwitch 6450, 6350

show [stacking] interfaces [*slot*[/*port*[-*port2*]]] counters
OmniSwitch 6450, 6350

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

OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] collisions
OmniSwitch 6450, 6350

show [stacking] interfaces [*slot*[/*port*[-*port2*]]] status
OmniSwitch 6450, 6350

show interfaces [*slot* | *slot*/*port*[-*port2*]*]* port
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] ifg
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] flood rate [broadcast | multicast | unknown-unicast]
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] traffic
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper}
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} status
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} flow control
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} pause
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} capability
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} accounting
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} counters
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} counters errors
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} collisions
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} traffic
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} port
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} flood rate
OmniSwitch 6450, 6350

show interfaces [*slot*[/*port*[-*port2*]]] hybrid {fiber |copper} ifg
OmniSwitch 6450, 6350

interfaces [*slot* | *slot*/*port***[**-*port2***]**] violation-recovery-time {seconds | default}
interfaces {*slot* | *slot*/*port***[**-*port2***]**} violation-recovery-time default
OmniSwitch 6450, 6350

interfaces [*slot* | *slot*/*port*[-*port2*]] violation-recovery-maximum *max_attempts*
interfaces {*slot* | *slot*/*port*[-*port2*]} violation-recovery-maximum default
OmniSwitch 6450, 6350

interface violation-recovery-trap {enable | disable}
OmniSwitch 6450, 6350

interfaces {*slot* | *slot*/*port*[-*port2*]} clear-violation-all
OmniSwitch 6450, 6350

show interfaces violation-recovery

OmniSwitch 6450, 6350

link-fault-propagation group *num*
no link-fault-propagation group *num*
OmniSwitch 6450, 6350

link-fault-propagation group *num* admin-status {enable | disable}
OmniSwitch 6450, 6350

link-fault-propagation group *num* source {port *slot/port* [-*port2*] | linkagg *aggid* [-*aggid2*]}
no link-fault-propagation group *num* source {port *slot/port* [-*port2*] | linkagg *aggid* [-*aggid2*]}
OmniSwitch 6450, 6350

link-fault-propagation group num destination {port *slot/port[-port2]* | linkagg *agg_id[-agg_id2]*}
no link-fault-propagation group num destination {port *slot/port[-port2]* | linkagg *agg_id[-agg_id2]*}
OmniSwitch 6450, 6350

link-fault-propagation group *num* wait-to-shutdown *seconds*
OmniSwitch 6450, 6350

show link-fault-propagation group *num*
OmniSwitch 6450, 6350

show interfaces [*slot* | *slot*/*port*[-*port2*]] transceiver [ddm | w-low | w-high | a-low | a-high | actual]
OmniSwitch 6450, 6350

show interfaces [*slot* | *slot*/*port*[-*port2*]] eee
OmniSwitch 6450

show interfaces ptp
OmniSwitch 6450 (OS6450-P10S and OS6450-U24S only)

show interfaces [*slot* | *slot*/*port*[-*port2*]] ptp-statistics
OmniSwitch 6450 (OS6450-P10S and OS6450-U24S only)

Port Mobility Commands

vlan *vid* dhcp mac *mac_address*
vlan *vid* no dhcp mac *mac_address*
OmniSwitch 6450, 6350

vlan *vid* dhcp mac range *low_mac_address high_mac_address*
vlan *vid* no dhcp mac range *low_mac_address*
OmniSwitch 6450, 6350

vlan *vid* dhcp port *slot/port*
vlan *vid* no dhcp port *slot/port*
OmniSwitch 6450, 6350

vlan *vid* dhcp generic
vlan *vid* no dhcp generic
OmniSwitch 6450, 6350

vlan *vid* mac *mac_address*
vlan *vid* no mac *mac_address*
OmniSwitch 6450, 6350

vlan *vid* mac range *low_mac_address high_mac_address*
vlan *vid* no mac range *low_mac_address*
OmniSwitch 6450, 6350

vlan *vid* ip *ip_address* [*subnet_mask*]
vlan *vid* no ip *ip_address* [*subnet_mask*]
OmniSwitch 6450, 6350

vlan *vid* protocol {ip-e2 | ip-snap | decnet | appletalk | ethertype *type* | dsapssap *dsap/ssap* | snap *snaptype*}
vlan *vid* no protocol {ip-e2 | ip-snap | decnet | appletalk | ethertype *type* | dsapssap *dsap/ssap* | snap *snaptype*}
OmniSwitch 6450, 6350

vlan *vid* port *slot/port*
vlan *vid* no port *slot/port*
OmniSwitch 6450, 6350

vlan port mobile *slot/port* [bpdu ignore {enable | disable}]
vlan no port mobile *slot/port*
OmniSwitch 6450, 6350

vlan port *slot/port* default vlan restore {enable | disable}
OmniSwitch 6450, 6350

vlan port *slot/port* default vlan {enable | disable}
OmniSwitch 6450, 6350

vlan port *slot/port* authenticate {enable | disable}
OmniSwitch 6450, 6350

vlan port *slot/port* 802.1x {enable | disable}
OmniSwitch 6450, 6350

show vlan [*vid*] rules
OmniSwitch 6450, 6350

show vlan port mobile [*slot/port*]
OmniSwitch 6450, 6350

VLAN Management Commands

vlan *vid* [enable | disable] [name *description*]
no vlan *vid*
OmniSwitch 6450, 6350

vlan *vid* [1x1 | flat] stp {enable | disable}
OmniSwitch 6450, 6350

vlan *vid* mobile-tag {enable | disable}
OmniSwitch 6450, 6350

vlan *vid* port default {*slot/port* | *link_agg_num*}
vlan *vid* no port default {*slot/port* | *link_agg_num*}
OmniSwitch 6450, 6350

vlan {*vid1***[-***vid2***] | ipmvlan** *ipmvlan-id***} source-learning {enable | disable}**
OmniSwitch 6450, 6350

show vlan [*vid*]
OmniSwitch 6450, 6350

show vlan [*vid*] port [*slot/port* | *link_agg*]
OmniSwitch 6450, 6350

show vlan router mac status
OmniSwitch 6450, 6350

show vlan gvrp [*vlan-id* | *vlan-range*]
OmniSwitch 6450

show vlan ipmvlan [*ipmvlan-id* | *ipmvlan-id1-ipmvlan-id2***]**
OmniSwitch 6450, 6350

GVRP Commands

gvrp
no gvrp
OmniSwitch 6450

gvrp **{linkagg** *agg_num* | **port** *slot/port***}**
no gvrp **{linkagg** *agg_num* | **port** *slot/port***}**
OmniSwitch 6450

gvrp transparent switching
no gvrp transparent switching
OmniSwitch 6450

gvrp maximum vlan *vlanlimit*
OmniSwitch 6450

no gvrp registration **{linkagg** *agg_num* | **port** *slot/port***}**

OmniSwitch 6450

gvrp applicant {participant | non-participant | active} **{linkagg** *agg_num* | **port** *slot/port***}**
no gvrp applicant **{linkagg** *agg_num* | **port** *slot/port***}**
OmniSwitch 6450

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***}**
OmniSwitch 6450

no gvrp restrict-vlan-registration **{linkagg** *agg_num* | **port** *slot/port***}** *vlan-list*
OmniSwitch 6450

no gvrp restrict-vlan-advertisement {**linkagg** *agg_num* | **port** *slot/port***}** *vlan-list*
OmniSwitch 6450

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*
OmniSwitch 6450

clear gvrp statistics [**linkagg** *agg_num* | **port** *slot/port]*
OmniSwitch 6450

show gvrp statistics **[linkagg** *agg_num* | **port** *slot/port***]**
OmniSwitch 6450

show gvrp last-pdu-origin **{linkagg** *agg_num* | **port** *slot/port***}**
OmniSwitch 6450

show gvrp configuration
OmniSwitch 6450

show gvrp configuration **port**
OmniSwitch 6450

show gvrp configuration **{linkagg** *agg_num* | **port** *slot/port***}**
OmniSwitch 6450

show gvrp timer [[join | leave | leaveall] {**linkagg** *agg_num* | **port** *slot/port*}**]**
OmniSwitch 6450

MVRP Commands

vlan registration-mode {gvrp | mvrp}
OmniSwitch 6450, 6350

mvrp **{enable** | **disable}**
OmniSwitch 6450, 6350

mvrp port *slot/port* [– *port2*] {enable | disable}
OmniSwitch 6450, 6350

mvrp linkagg *agg_num* [-*agg_num2*] {enable | disable}
OmniSwitch 6450, 6350

mvrp transparent-switching {enable | disable}
OmniSwitch 6450, 6350

mvrp maximum vlan *vlanlimit*
OmniSwitch 6450, 6350

mvrp {port *slot/port* [– *port2*] | linkagg *agg_num* [-*agg_num2*]} registration {normal | fixed |
forbidden}
OmniSwitch 6450, 6350

mvrp {port *slot/port* [– *port2*] | linkagg *agg_num* [-*agg_num2*]} applicant {participant |
non-participant | active}
OmniSwitch 6450, 6350

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer join** *timer-value*
OmniSwitch 6450, 6350

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer leave** *timer-value*
OmniSwitch 6450, 6350

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer leaveall** *timer-value*
OmniSwitch 6450, 6350

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer periodic-timer** *timer-value*
OmniSwitch 6450, 6350

mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} periodic-transmission {enable | disable}**
OmniSwitch 6450, 6350

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
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

show mvrp configuration
OmniSwitch 6450, 6350

show mvrp port {*slot/port* [-*port2*]} [enabled | disabled]
OmniSwitch 6450, 6350

show mvrp linkagg [*agg_num* [-*agg_num2*]} [enabled | disabled]
OmniSwitch 6450, 6350

show mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]} timer {join | leave | leaveall | periodic-timer}**
OmniSwitch 6450, 6350

show mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]}** statistics
OmniSwitch 6450, 6350

show mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]}** last-pdu-origin
OmniSwitch 6450, 6350

show vlan registration-mode
OmniSwitch 6450, 6350

show mvrp {port *slot/port* **[–** *port2***] | linkagg** *agg_num* **[-***agg_num2***]}** vlan-restrictions
OmniSwitch 6450, 6350

show vlan mvrp [vlan-id | vlan-range]
OmniSwitch 6450, 6350

mvrp **[**port *slot/port* [–*port2*] | linkagg *agg_num* [-*agg_num2*]**]** clear-statistics
OmniSwitch 6450, 6350

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]
OmniSwitch 6450

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
OmniSwitch 6450

ethernet-service {svlan | ipmvlan} *svid1***[**-*svid2***]** source-learning {enable| disable}
OmniSwitch 6450

ethernet-service service-name *service-name* {svlan | ipmvlan} *svid*
no ethernet-service service-name *service-name* {svlan | ipmvlan} *svid*
OmniSwitch 6450

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}
OmniSwitch 6450

ethernet-service nni {slot/port1[-port2] | agg_num} **[tpid** *value*] [{stp | gvrp | mvrp} legacy-bpdu {enable | disable}] [transparent-bridging {enable | disable}]
OmniSwitch 6450

ethernet-service sap *sapid* service-name *service-name*
no ethernet-service sap sapid
OmniSwitch 6450

ethernet-service sap sapid uni {slot/port1[-port2] | **linkagg** agg_num}
ethernet-service sap sapid no uni {slot/port1[-*port2*] | **linkagg** agg_num}
OmniSwitch 6450

ethernet-service sap sapid cvlan {**all** | *cvid* | *cvid1-cvid2* | **untagged**}
ethernet-service sap sapid no cvlan {**all** | *cvid* | *cvid1-cvid2* | **untagged**}
OmniSwitch 6450

ethernet-service sap-profile *sap-profile-name*
no ethernet-service sap-profile *sap-profile-name*
OmniSwitch 6450

ethernet-service sap *sapid* sap-profile *sap-profile-name*
OmniSwitch 6450

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*
OmniSwitch 6450

ethernet-service uni {slot/port1[-port2] | agg_num} **uni-profile** uni-profile-name
OmniSwitch 6450

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*
OmniSwitch 6450

ethernet-service mac-tunneling {enable | disable}
OmniSwitch 6450

ethernet-service untagged-cvlan-insert {enable | disable}
OmniSwitch 6450

ethernet-service sap *sap_id* uni {*slot/port* | **linkagg** agg_num}untagged-cvlan *cvlan_id*
OmniSwitch 6450

ethernet-service svlan svid1[-svid2] mac-tunneling {enable | disable} [name description]
OmniSwitch 6450

show ethernet-service custom-L2-protocol custom-L2-protocol
OmniSwitch 6450

show ethernet-service mode
OmniSwitch 6450

show ethernet-services vlan [svid1-**[**svid2]]
OmniSwitch 6450

show ethernet-service [service-name *service-name* | **svlan** svid]
OmniSwitch 6450

show ethernet-services sap [*sapid*]
OmniSwitch 6450

show ethernet-services port {*slot/port* | **linkagg** agg_num}
OmniSwitch 6450

show ethernet-services nni [*slot/port* | **linkagg** agg_num]
OmniSwitch 6450

show ethernet-services nni [*slot/port* | **linkagg** agg_num] l2pt-statistics
OmniSwitch 6450

clear ethernet-services nni [**linkagg** agg_num | *slot/port* | *port range*] l2pt-statistics
OmniSwitch 6450

show ethernet-service uni [*slot/port* | **linkagg** agg_num]
OmniSwitch 6450

show ethernet-service uni [*slot/port* | **linkagg** agg_num] l2pt-statistics
OmniSwitch 6450

clear ethernet-service uni [**linkagg** agg_num | *slot/port* | *port range*] l2pt-statistics
OmniSwitch 6450

show ethernet-service uni-profile [*uni-profile-name*]
OmniSwitch 6450

show ethernet-service uni-profile [*uni-profile-name*] l2pt-statistics
OmniSwitch 6450

show ethernet-service untagged-cvlan-insert
OmniSwitch 6450

clear ethernet-service uni-profile [**uni profile name]** l2pt-statistics
OmniSwitch 6450

show ethernet-service sap-profile *sap-profile-name*
OmniSwitch 6450

loopback-test *profile_name* destination-mac *dest_address* loopback-port *slot/port [*source-mac *src_address]* [vlan *vlan_id]* type inward
loopback-test *profile_name* destination-mac *dest_address* loopback-port *slot/port [*source-mac *src_address]* vlan *vlan_id* type outward [sap *sap_id*]
loopback-test *profile_name* {enable | disable}
no loopback-test *profile_name*
OmniSwitch 6450

show loopback-test [*profile_name*]
OmniSwitch 6450

Ethernet OAM Commands

ethoam vlan vlanid-list primary-vlan vlan-id
no ethoam vlan vlanid-list
OmniSwitch 6450

ethoam domain *name* format {none | **dnsname** | **mac-address-unit** | **string**} level *num*
no ethoam domain *name*
OmniSwitch 6450

ethoam domain *name* **mhf {none** | **explicit** | **default}**
OmniSwitch 6450

ethoam domain name id-permission {none | chassisid}

OmniSwitch 6450

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*
OmniSwitch 6450

ethoam association ma-name domain md-name mhf {none |default | explicit | defer}
OmniSwitch 6450

ethoam association ma-name domain md-name id-permission {none | chassisid | defer}
OmniSwitch 6450

ethoam association *association_name* **domain {***domain_name* | *mac_address***} ccm-interval {interval-invalid | interval100ms | interval1s** | **interval10s** | **interval1m** | **interval10m}**
OmniSwitch 6450

ethoam association *association_name* domain **{***domain_name* | *mac_address***}**
endpoint-list *mep_id*[*-mep_id2***]**
no ethoam association *association_name* domain **{***domain_name* | *mac_address***}**
endpoint-list *mep_id*[*-mep_id2***]**
OmniSwitch 6450

ethoam association *association_name* domain **{***domain_name* | *mac_address***}**
allowed-cvlan-list *num* [*-num2***]**
no ethoam association *association_name* domain **{***domain_name* | *mac_address***}**
allowed-cvlan-list *num* [*-num2***]**
OmniSwitch 6450

clear ethoam statistics [domain domain association association endpoint mep-id]
OmniSwitch 6450

ethoam default-domain level *num*
no ethoam default-domain
OmniSwitch 6450

ethoam default-domain mhf {none | default | explicit}
no ethoam default-domain
OmniSwitch 6450

ethoam default-domain id-permission {none | chassisid}
no ethoam default-domain
OmniSwitch 6450

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
OmniSwitch 6450

ethoam endpoint *mep-id* domain *md_name* association *ma_name* direction {up | down} {port {*slot/port* | virtual | linkagg *agg_id*} [primary-vlan *vlan_id* | *cvlan cvlan_id*]
no ethoam endpoint mep-id domain md_name association ma_name
OmniSwitch 6450

ethoam endpoint *mep_id* domain **{***domain_name* | *mac_address***}** association *association_name*
admin-state {enable | disable}
OmniSwitch 6450

ethoam endpoint *mep_id* domain **{***domain_name* | *mac_address***}** association *association_name*
ccm {enable | disable}
OmniSwitch 6450

ethoam endpoint *mep_id* domain **{***domain_name* | *mac_address***}** association *association_name* priority *ccm_ltm_priority*
OmniSwitch 6450

ethoam endpoint *mep_id* domain **{***domain_name* | *mac_address***}** association *association_name* lowest-defect-priority *lowest_priority_defect*
OmniSwitch 6450

ethoam endpoint *mep-id* domain *md-name* association *ma-name* direction {up | down} {port *slot/port* | linkagg *id*} [primary-vlan *vlan-id*]
OmniSwitch 6450

ethoam endpoint *mep-id* domain *md-name* association *ma-name* ctag-priority {copy-outer-to-inner | *num*}
OmniSwitch 6450

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}]
OmniSwitch 6450

ethoam linktrace {target-macaddress *mac_address* **| target-endpoint** *tar_mep_id***} source-endpoint** *src_mep_id* **domain {***domain_name* | *mac_address***} association** *association_name* **[flag {fdbonly | fdb-mpdb}] [hop-count** *hop_count***]**
OmniSwitch 6450

ethoam fault-alarm-time *centiseconds* **endpoint** *endpoint_id* **domain {***domain_name* | *mac_address***}**
association *association_name*
no ethoam fault-alarm-time endpoint *endpoint_id* **domain {***domain_name* | *mac_address***}**
association *association_name*
OmniSwitch 6450

ethoam fault-reset-time *centiseconds* **endpoint** *endpoint_id* **domain** {*mac_address* | *domain_name}* **association** *association_name*
no ethoam fault-reset-time endpoint *endpoint_id* **domain** {*mac_address* | *domain_name}* **association** *association_name*
OmniSwitch 6450

ethoam one-way-delay {target-endpoint t-mepid | target-macaddress mac_add} source-endpoint s-mepid domain domain association association [vlan- priority vlan-priority]
OmniSwitch 6450

ethoam two-way-delay {target-endpoint t-mepid | target-macaddress mac_add} source-endpoint s-mepid domain domain association association [vlan- priority vlan-priority]
OmniSwitch 6450

clear ethoam {one-way-delay-table | two-way-delay-table}
OmniSwitch 6450

show ethoam
OmniSwitch 6450

show ethoam domain *md-name*
OmniSwitch 6450

show ethoam domain *md-name* **association** *ma-name*
OmniSwitch 6450

show ethoam domain *md-name* **association** *ma-name* **endpoint** *mep-id*
OmniSwitch 6450

show ethoam default-domain [primary-vlan *vlan_id***]**
OmniSwitch 6450

show ethoam default-domain configuration
OmniSwitch 6450

show ethoam remote-endpoint domain m*d_name* **association m***a_name* **endpoint** *smep-id* **[remote-mep** *rmep-id***]**
OmniSwitch 6450

show ethoam cfmstack [port{*slot/port* | virtual} | **linkagg** *agg_num***]**
OmniSwitch 6450

show ethoam linktrace-reply domain *d-name* **association** *a-name* **endpoint** *s-mepid* **tran-id** *num*
OmniSwitch 6450

show ethoam linktrace-tran-id domain {*domain_name* | *mac_address***} association** *association_name* **endpoint** *mep_id*
OmniSwitch 6450

show ethoam vlan vlan-id
OmniSwitch 6450

show ethoam statistics domain {*domain_name* | *mac_address***} [association** *association_name***] [end-point** *endpoint_id***]**
OmniSwitch 6450

show ethoam config-error [vlan vid] [{port slot/port | linkagg aggid}]
OmniSwitch 6450

show ethoam one-way-delay domain domain association association endpoint s-mepid [mac-address mac-add]
OmniSwitch 6450

show ethoam two-way-delay domain domain association association endpoint s-mepid [mac-address mac-add]
OmniSwitch 6450

Service Assurance Agent Commands

saa string [descr description] [interval interval]
no *saa string*
OmniSwitch 6450

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]
OmniSwitch 6450

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]
OmniSwitch 6450

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]
OmniSwitch 6450

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]
OmniSwitch 6450

saa string start [at yyyy-mm-dd,hh:mm:ss.ds]
OmniSwitch 6450

saa string stop [never | at yyyy-mm-dd,hh:mm:ss.ds]
OmniSwitch 6450

saa jitter-calculation {default|enhanced}
OmniSwitch 6450

show saa config
OmniSwitch 6450

show saa [string | {descr description}]
OmniSwitch 6450

show saa [string] type {mac-ping | ip-ping | ethoam-loopback | ethoam-two-way-delay} config
OmniSwitch 6450

show saa **[***string***]** *statistics [aggregate | history]*
OmniSwitch 6450

LINK OAM Commands

efm-oam {enable | disable}
OmniSwitch 6450

efm-oam port *slot/port* **[**-*port2***] status {enable | disable}**
OmniSwitch 6450

efm-oam port *slot/port***[**-*port2***]** mode {*active* | *passive*}
OmniSwitch 6450

efm-oam port *slot/port***[**-*port2***] keepalive-interval** *seconds*
OmniSwitch 6450

efm-oam port *slot/port*[-*port2*] hello-interval *seconds*
OmniSwitch 6450

efm-oam port *slot/port*[-*port2*] remote-loopback {process | ignore}
OmniSwitch 6450

efm-oam port *slot/port* remote-loopback {start | stop}
OmniSwitch 6450

efm-oam port *slot/port*[-*port2*] propagate-events {critical-event | dying-gasp} {enable | disable}
OmniSwitch 6450

efm-oam port *slot/port*[-*port2*] errored-frame-period [threshold *threshold_symbols*] [window *window_frames*] [notify {enable | disable}]
OmniSwitch 6450

efm-oam port *slot/port*[-*port2*] errored-frame [threshold *threshold_symbols*] [window *window_seconds*] [notify {enable | disable}]
OmniSwitch 6450

efm-oam port *slot/port*[-*port2*] errored-frame-seconds-summary [threshold *threshold_seconds*] [window *window_seconds*] [notify {enable | disable}]
OmniSwitch 6450

efm-oam multiple-pdu-count *count*
OmniSwitch 6450

efm-oam port *slot/port* l1-ping [num-frames *number*] [delay *milliseconds*] [start]
OmniSwitch 6450

show efm-oam configuration
OmniSwitch 6450

show efm-oam port [*slot*/*port1*-*port2*] [enable | disable] [active | passive]
OmniSwitch 6450

show efm-oam port *slot/port* detail
OmniSwitch 6450

show efm-oam **port** *slot*/*port*[-*port2*] statistics
show efm-oam **port** statistics
OmniSwitch 6450

show efm-oam port *slot*/*port* remote detail
OmniSwitch 6450

show efm-oam port *slot*/*port* history [log-type { link-fault | errored-frame | errored-frame-period | errored-frame-seconds | dying-gasp | critical}]
OmniSwitch 6450

show efm-oam port *slot*/*port* l1-ping detail
OmniSwitch 6450

clear efm-oam statistics *port slot/port*[-*port2*]
OmniSwitch 6450

clear efm-oam log-history *port slot/port*[-*port2*]
OmniSwitch 6450

UDLD Commands

udld {enable | disable}

OmniSwitch 6450, 6350

udld port slot/port[-*port2*] {enable | disable}
OmniSwitch 6450, 6350

udld port [slot/port[-*port2*]] mode {normal | aggressive}
OmniSwitch 6450, 6350

udld port [slot/port[-*port2*]] probe-timer seconds
no udld port [slot/port[-*port2*]] probe-timer
OmniSwitch 6450, 6350

udld port [slot/port[-*port2*]] echo-wait-timer seconds
no udld port [slot/port[-*port2*]] echo-wait-timer
OmniSwitch 6450, 6350

clear udld statistics [port slot/port]
OmniSwitch 6450, 6350

interfaces slot/port[-*port2*] **clear-violation-all**
OmniSwitch 6450, 6350

show udld configuration
OmniSwitch 6450, 6350

show udld configuration port [slot/port]
OmniSwitch 6450, 6350

show udld statistics port slot/port
OmniSwitch 6450, 6350

show udld neighbor port slot/port
OmniSwitch 6450, 6350

show udld status port [slot/port]
OmniSwitch 6450, 6350

Port Mapping Commands

OmniSwitch 6450, 6350

port mapping *session_id* {enable | disable}
no port mapping *session_id*
OmniSwitch 6450, 6350

port mapping *session_id* {**unidirectional | bidirectional}**
OmniSwitch 6450, 6350

port mapping port_mapping_session id dynamic-proxy-arp {enable | **disable}**
OmniSwitch 6450, 6350

show port mapping [*session_id*] **status**
OmniSwitch 6450, 6350

show port mapping [*session_id*]
OmniSwitch 6450, 6350

IP Commands

ip interface *name* [address *ip_address*] [mask *subnet_mask*] [admin [enable | disable]] [vlan *vid*] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [eth2 | snap] [primary | no primary] local-host-dbcast [enable | disable]
no ip interface *name*
OmniSwitch 6450, 6350

no ip interface *name*
OmniSwitch 6450, 6350

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]
OmniSwitch 6450, 6350

ip interface *dhcp-client* [vlan *vid ifindex id*] [*vsi-accept-filter filter-string* | **server-preference**] [firewall-vlan *vid***]**[release | renew] [option-60 opt60_string] [admin {enable | disable}]
no ip interface *dhcp-client*
ip interface *dhcp-client no server-preference*
OmniSwitch 6450, 6350

ip router primary-address *ip_address*
OmniSwitch 6450, 6350

ip router router-id *ip_address*
OmniSwitch 6450, 6350

ip static-route *ip_address* [mask *mask*] gateway *gateway* [metric *metric*]
no ip static-route *ip_address* [mask *mask*] gateway *ip_address* [metric *metric*]
OmniSwitch 6450, 6350

ip route-pref {static | rip | ebgp | ibgp} *value*
OmniSwitch 6450, 6350

ip default-ttl *hops*
OmniSwitch 6450, 6350

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 *string*]
OmniSwitch 6450, 6350

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*]
OmniSwitch 6450, 6350

ip directed-broadcast {on | off | controlled}
OmniSwitch 6450, 6350

ip directed-broadcast allow source-ip *ip_address* [mask *subnet_mask*] [destination-ip *ip_address* [mask *subnet_mask*] | vlan *vlan_id*]
no ip directed-broadcast source-ip *ip_address*
OmniSwitch 6450, 6350

ip directed-broadcast clear
OmniSwitch 6450, 6350

ip service {all | *service_name* | port *service_port*}
no ip service {all | *service_name* | port *service_port*}
OmniSwitch 6450, 6350

ip tables {extend | default}
OmniSwitch 6350

ip redist {local | static | rip} into {rip} route-map *route-map-name* [status {enable | disable}]
no ip redist {local | static | rip} into {rip} [route-map *route-map-name*]
OmniSwitch 6450, 6350

ip access-list *access-list-name*
no ip access-list access-list-name
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

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]**

OmniSwitch 6450, 6350

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** {*access-list-name* | *ipv6_address/prefixLen* **[redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]**
OmniSwitch 6450, 6350

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]}**
OmniSwitch 6450, 6350

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]}
OmniSwitch 6450, 6350

ip route-map *route-map-name* **[sequence-number** *number***] match tag** *tag-number*
no ip route-map *route-map-name* **[sequence-number** *number***] match tag** *tag-number*
OmniSwitch 6450, 6350

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
OmniSwitch 6450, 6350

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
OmniSwitch 6450, 6350

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]
OmniSwitch 6450, 6350

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}]
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

arp *ip_address hardware_address* [alias]

no arp *ip_address* [alias]
OmniSwitch 6450, 6350

clear arp-cache
OmniSwitch 6450, 6350

ip dos arp-poison restricted-address ip_address
no ip dos arp-poison restricted-address ip_address
OmniSwitch 6450, 6350

arp filter *ip_address* [mask *ip_mask*] [*vid*] [sender | target] [allow | block]
no arp filter *ip_address*
OmniSwitch 6450, 6350

clear arp-cache
OmniSwitch 6450, 6350

ip arp-limit default
OmniSwitch 6450

ip arp-limit extend
OmniSwitch 6450

icmp type *type* code *code* {{enable | disable} | min-pkt-gap *gap*}
OmniSwitch 6450, 6350

icmp unreachable [net-unreachable | host-unreachable | protocol-unreachable | port-unreachable] {{enable | disable} | min-pkt-gap *gap*}
OmniSwitch 6450, 6350

icmp echo [request | reply] {{enable | disable} | min-pkt-gap *gap*}
OmniSwitch 6450, 6350

icmp timestamp [request | reply] {{enable | disable} | min-pkt-gap *gap*}
OmniSwitch 6450, 6350

icmp add-mask [request | reply] {{enable | disable} | min-pkt-gap *gap*}
OmniSwitch 6450, 6350

icmp messages {enable | disable}
OmniSwitch 6450, 6350

twamp server [port *port-number*] [inactivity-timeout *mins*] [allowed-client *ipv4-address ip-mask*]
no twamp server
OmniSwitch 6450

ip dos scan close-port-penalty *penalty_value*
OmniSwitch 6450, 6350

ip dos scan tcp open-port-penalty *penalty_value*
OmniSwitch 6450, 6350

ip dos scan udp open-port-penalty *penalty_value*
OmniSwitch 6450, 6350

ip dos scan threshold *threshold_value*
OmniSwitch 6450, 6350

ip dos trap {enable | disable}
OmniSwitch 6450, 6350

ip dos scan decay *decay_value*
OmniSwitch 6450, 6350

show ip traffic
OmniSwitch 6450, 6350

show ip interface [*name* | vlan *vlan id* | *dhcp-client*]
OmniSwitch 6450, 6350

show ip interface cvlan
OmniSwitch 6450, 6350

show ip managed-interface
OmniSwitch 6450, 6350

show ip route [summary]
OmniSwitch 6450, 6350

show ip route-pref
OmniSwitch 6450, 6350

show ipv6 redist [rip]
OmniSwitch 6450, 6350

show ip access-list [*access-list-name*]
OmniSwitch 6450, 6350

show ip route-map [*route-map-name*]
OmniSwitch 6450, 6350

show ip router database [protocol *type* | gateway *ip_address* | dest {*ip_address/*prefixLen | *ip_address*}]
OmniSwitch 6450, 6350

show ip config
OmniSwitch 6450, 6350

show ip protocols
OmniSwitch 6450, 6350

show ip service
OmniSwitch 6450, 6350

show arp [*ip_address* | *hardware_address*]
OmniSwitch 6450, 6350

show ip dynamic-proxy-arp
OmniSwitch 6450, 6350

show arp filter [*ip_address*]
OmniSwitch 6450, 6350

show icmp control
OmniSwitch 6450, 6350

show icmp [statistics]
OmniSwitch 6450, 6350

show twamp server info
OmniSwitch 6450

show twamp server connections [client *ipv4-address*]
OmniSwitch 6450

show tcp statistics
OmniSwitch 6450, 6350

show tcp ports
OmniSwitch 6450, 6350

show udp statistics
OmniSwitch 6450, 6350

show udp ports
OmniSwitch 6450, 6350

show ip dos config
OmniSwitch 6450, 6350

show ip dos statistics
OmniSwitch 6450, 6350

show ip dos arp-poison
OmniSwitch 6450, 6350

IPv6 Commands

ipv6 interface if_name vlan vid [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
OmniSwitch 6450, 6350

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***}**
OmniSwitch 6450, 6350

ipv6 dad-check *ipv6_address if_name*
OmniSwitch 6450, 6350

ipv6 hop-limit *value*
no ipv6 hop-limit
OmniSwitch 6450, 6350

ipv6 pmtu-lifetime *time*
OmniSwitch 6450, 6350

ipv6 host *name ipv6_address*
no ipv6 host *name ipv6_address*
OmniSwitch 6450, 6350

ipv6 neighbor stale-lifetime *stale-lifetime*
OmniSwitch 6450, 6350

ipv6 neighbor *ipv6_address hardware_address if_name slot/port*
no ipv6 neighbor *ipv6_address if_name*
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

ipv6 route *ipv6_prefix/prefix_length ipv6_address* **[***if_name***]**
no ipv6 route *ipv6_prefix/prefix_length ipv6_address* **[***if_name]*
OmniSwitch 6450, 6350

ipv6 static-route *ipv6_prefix/prefix_length* gateway *ipv6_address* [*if_name*]
[metric *metric*]
no ipv6 static-route *ipv6_prefix/prefix_length* gateway *ipv6_address* [*if_name*]
OmniSwitch 6450, 6350

ipv6 route-pref {static | rip} *value*
OmniSwitch 6450, 6350

ipv6 ra-filter vlan vlan-number [{trusted-port slot/port | trusted-linkagg id}]
OmniSwitch 6450, 6350

ipv6 ra-filter clear counters
OmniSwitch 6450, 6350

ping6 {*ipv6_address* | *hostname*} *[if_name]* [count *count*] [size *data_size*]
[interval *seconds*]
OmniSwitch 6450, 6350

traceroute6 {ipv6_address | hostname} [if_name] [max-hop *hop_count*]
[wait-time time] [port port_number] [probe-count probe]
OmniSwitch 6450, 6350

show ipv6 hosts [substring]
OmniSwitch 6450, 6350

show ipv6 icmp statistics [if_name]
OmniSwitch 6450, 6350

show ipv6 interface [if_name | loopback]
OmniSwitch 6450, 6350

show ipv6 pmtu table
OmniSwitch 6450, 6350

clear ipv6 pmtu table
OmniSwitch 6450, 6350

show ipv6 neighbors [ipv6_prefix/prefix_length | if_name | hw hardware_address | static]
OmniSwitch 6450, 6350

clear ipv6 neighbors
OmniSwitch 6450, 6350

show ipv6 prefixes
OmniSwitch 6450, 6350

show ipv6 routes [ipv6_prefix/prefix_length | static]
OmniSwitch 6450, 6350

show ipv6 route-pref
OmniSwitch 6450, 6350

show iv6p router database [protocol *type* | gateway *ipv6_address* | dest *ipv6_prefix/prefix_length*]
OmniSwitch 6450, 6350

show ipv6 tcp ports
OmniSwitch 6450, 6350

show ipv6 traffic [if_name]
OmniSwitch 6450, 6350

clear ipv6 traffic
OmniSwitch 6450, 6350

show ipv6 udp ports
OmniSwitch 6450, 6350

show ipv6 information
OmniSwitch 6450, 6350

show ipv6 ra-filter vlan [number]
OmniSwitch 6450, 6350

show ipv6 ra-filter counters
OmniSwitch 6450, 6350

ipv6 redist {local | static | rip} into {rip} route-map *route-map-name* [status {enable | disable}]
OmniSwitch 6450, 6350

ipv6 access-list *access-list-name*
no ipv6 access-list access-list-name
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

show ipv6 redist [rip]
OmniSwitch 6450, 6350

show ip access-list [*access-list-name*]
OmniSwitch 6450, 6350

ipv6 load rip
OmniSwitch 6450

ipv6 rip status {enable | disable}
OmniSwitch 6450

ipv6 rip invalid-timer seconds
OmniSwitch 6450

ipv6 rip garbage-timer seconds
OmniSwitch 6450

ipv6 rip holddown-timer seconds
OmniSwitch 6450

ipv6 rip jitter value
OmniSwitch 6450

ipv6 rip route-tag value
OmniSwitch 6450

ipv6 rip update-interval seconds
OmniSwitch 6450

ipv6 rip triggered-sends {all | updated-only | none}
OmniSwitch 6450

ipv6 rip interface if_name
[no] ipv6 rip interface if_name
OmniSwitch 6450

ipv6 rip interface if_name metric value
OmniSwitch 6450

ipv6 rip interface if_name recv-status {enable | disable}
OmniSwitch 6450

ipv6 rip interface if_name send-status {enable | disable}
OmniSwitch 6450

ipv6 rip interface if_name horizon {none | split-only | poison}
OmniSwitch 6450

show ipv6 rip
OmniSwitch 6450

show ipv6 rip interface [if_name]
OmniSwitch 6450

show ipv6 rip peer [ipv6_addresss]
OmniSwitch 6450

show ipv6 rip routes [dest <ipv6_prefix/prefix_length>] | [gateway <ipv6_addr>] | [detail <ipv6 prefix/prefix_length>]
OmniSwitch 6450

RDP Commands

ip router-discovery {enable | disable}
OmniSwitch 6450, 6350

ip router-discovery interface *name* [enable | disable]
no router-discovery interface *name*
OmniSwitch 6450, 6350

ip router-discovery interface *name* advertisement-address {all-systems-multicast | broadcast}
OmniSwitch 6450, 6350

ip router-discovery interface *name* max-advertisement-interval *seconds*
OmniSwitch 6450, 6350

ip router-discovery interface *name* min-advertisement-interval *seconds*
OmniSwitch 6450, 6350

ip router-discovery interface *name* advertisement-lifetime *seconds*
OmniSwitch 6450, 6350

ip router-discovery interface *name* preference-level *level*
OmniSwitch 6450, 6350

show ip router-discovery
OmniSwitch 6450, 6350

show ip router-discovery interface [*name*]
OmniSwitch 6450, 6350

DHCP Relay Commands

ip helper address *ip_address*
ip helper no address [*ip_address*]
OmniSwitch 6450, 6350

ip helper address *ip_address* vlan *vlan_id*
ip helper no address *ip_address* vlan *vlan_id*
OmniSwitch 6450, 6350

ip helper standard
OmniSwitch 6450, 6350

ip helper avlan only
OmniSwitch 6450, 6350

ip helper per-vlan only
OmniSwitch 6450, 6350

ip helper forward delay *seconds*
OmniSwitch 6450, 6350

ip helper maximum hops *hops*
OmniSwitch 6450, 6350

ip helper agent-information {enable | disable}
OmniSwitch 6450, 6350

ip helper agent-information policy {drop | keep | replace}
OmniSwitch 6450, 6350

ip helper pxe-support {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping trap-mode {default | reverse-enable | hardware | software}
OmniSwitch 6450, 6350

ip helper dhcp-snooping mac-address verification {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping option-82 data-insertion {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping option-82 data-insertion format [base-mac | system-name | user-string *string*]
OmniSwitch 6450, 6350

ip helper dhcp-snooping option-82 format ascii circuit-id {base-mac | system-name | vlan |
user-string *string* | *interface-alias* | *auto-interface-alias* | *cvlan} {delimiter character}*
no ip helper dhcp-snooping option-82 format ascii circuit-id
OmniSwitch 6450, 6350

ip helper dhcp-snooping option-82 format ascii remote-id {base-mac | system-name | vlan |
user-string *string* | *interface-alias* | *auto-interface-alias* | *cvlan} {delimiter character}*
no ip helper dhcp-snooping option-82 format ascii remote-id
OmniSwitch 6450, 6350

ip helper dhcp-snooping bypass option-82-check {enable | disable}
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

ip helper dhcp-snooping port *slot1*/*port1*[-*port1a*] {block | client-only | trust}
OmniSwitch 6450, 6350

ip helper dhcp-snooping linkagg *num* {block | client-only | trust| ip-source-filtering}
OmniSwitch 6450, 6350

ip helper dhcp-snooping port *slot1*/*port1*[-*port1a*] traffic-suppression {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping port *slot*/*port*[-*port1a*] ip-source-filter {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping binding {[enable | disable] | [*mac_address [***port** *slot/port | linkagg num]* **address** *ip_address* **vlan** *vlan_id*]}
no ip helper dhcp-snooping binding *mac_address [***port** *slot/port | linkagg num]* **address** *ip_address* **vlan** *vlan_id*
OmniSwitch 6450, 6350

ip helper dhcp-snooping ip-source-filter {vlan num [allow ip_address mask subnet_mask | port *slot*/*port* [-*port2*] | linkagg num} {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping port binding timeout *seconds*
OmniSwitch 6450, 6350

ip helper dhcp-snooping port binding action {purge | renew}
OmniSwitch 6450, 6350

ip helper dhcp-snooping binding persistency {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping ip-source-filter arp-allow {enable | disable}
OmniSwitch 6450, 6350

ip helper dhcp-snooping clear violation-counters {all | slot *num* | linkagg *num* | *slot/port* | *slot/port1-port2*}
OmniSwitch 6450, 6350

ip helper dhcp-snooping clear global-counters
OmniSwitch 6450, 6350

show ip helper dhcp-snooping global-counters
OmniSwitch 6450, 6350

ip helper dhcp-snooping clear isf-log
OmniSwitch 6450, 6350

ip helper dhcp-snooping clear isf-log
OmniSwitch 6450, 6350

ip helper boot-up {enable | disable}
OmniSwitch 6450, 6350

ip helper boot-up enable {BOOTP | DHCP}
OmniSwitch 6450, 6350

ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port* [*name***]}**
no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*}
OmniSwitch 6450, 6350

ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*} vlan *vlan_id*
no ip udp relay {BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*} vlan *vlan_id*

OmniSwitch 6450, 6350

dhcp-server {enable | disable}
OmniSwitch 6450, 6350

dhcp-server restart
OmniSwitch 6450, 6350

show dhcp-server leases [ip- address ip_address | mac-address mac_address] [type {static | dynamic }] [count]
OmniSwitch 6450, 6350

show dhcp-server statistics [packets | hosts | subnets | all]
OmniSwitch 6450, 6350

clear dhcp-server statistics
OmniSwitch 6450, 6350

show ip helper
OmniSwitch 6450, 6350

show ip helper stats
ip helper no stats
OmniSwitch 6450, 6350

show ip helper dhcp-snooping vlan
OmniSwitch 6450, 6350

show ip helper dhcp-snooping port
OmniSwitch 6450, 6350

show ip helper dhcp-snooping binding [port | ipaddress | linkagg]
OmniSwitch 6450, 6350

show ip udp relay service [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*]
OmniSwitch 6450, 6350

show ip udp relay [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*]
OmniSwitch 6450, 6350

show ip udp relay destination [BOOTP | NBDD | NBNSNBDD | DNS | TACACS | TFTP | NTP | *port*]
OmniSwitch 6450, 6350

show ip helper dhcp-snooping ip-source-filter {vlan | port | binding}
OmniSwitch 6450, 6350

ipv6 helper address *ipv6_address*
ipv6 helper no address [*ipv6_address*]
OmniSwitch 6450, 6350

ipv6 helper address *ipv6_address* vlan *vlan_id*
ipv6 helper no address *ipv6_address* vlan *vlan_id*
OmniSwitch 6450, 6350

ipv6 helper standard
OmniSwitch 6450, 6350

ipv6 helper per-vlan only
OmniSwitch 6450, 6350

ipv6 helper maximum hops *num*
OmniSwitch 6450, 6350

ipv6 helper dhcp-snooping {enable | disable}
OmniSwitch 6450, 6350

ipv6 helper dhcp-snooping vlan *vlan_id*
no ipv6 helper dhcp-snooping vlan *vlan_id*
OmniSwitch 6450, 6350

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 dhcp-snooping ip-source-filter {vlan num | port *slot*/*port*[-*port2*] | linkagg num} {enable | disable}
OmniSwitch 6450, 6350

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
OmniSwitch 6450, 6350

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
show ip helper dhcp-snooping ip-source-filter {port | vlan}
OmniSwitch 6450, 6350

show ip helper dhcp-snooping ip-source-filter binding
OmniSwitch 6450, 6350

RMON Commands

rmon probes {stats | history | alarm} [*entry-number*] {enable | disable}
OmniSwitch 6450, 6350

show rmon probes [stats | history | alarm] [*entry-number*]
OmniSwitch 6450, 6350

show rmon events [*event-number*]
OmniSwitch 6450, 6350

RIP Commands

ip load rip
OmniSwitch 6450

ip rip status {enable | disable}
OmniSwitch 6450

ip rip interface *interface_name*
no ip rip interface *interface_name*
OmniSwitch 6450

ip rip interface *interface_name* status {enable | disable}
OmniSwitch 6450

ip rip interface *interface_name* metric *value*
OmniSwitch 6450

ip rip interface *interface_name* send-version {none | v1 | v1compatible | v2}
OmniSwitch 6450

ip rip interface *interface_name* recv-version {v1 | v2 | both | none}
OmniSwitch 6450

ip rip force-holddowntimer *seconds*
OmniSwitch 6450

ip rip host-route
no ip rip host-route
OmniSwitch 6450

ip rip route-tag *value*
OmniSwitch 6450

ip rip interface *interface_name* auth-type {none | simple | md5}
OmniSwitch 6450

ip rip interface *interface_name* auth-key *string*
OmniSwitch 6450

ip rip update-interval *seconds*
OmniSwitch 6450

ip rip invalid-timer *seconds*
OmniSwitch 6450

ip rip garbage-timer *seconds*
OmniSwitch 6450

ip rip holddown-timer *seconds*
OmniSwitch 6450

show ip rip
OmniSwitch 6450

show ip rip routes **[***ip_address ip_mask***]**
OmniSwitch 6450

show ip rip interface **[***interface_name***]**
OmniSwitch 6450

show ip rip peer [*ip_address*]
OmniSwitch 6450

VRRP Commands

vrrp *vrid vlan_id* **[**enable | disable | on | off] [priority *priority*] [preempt | no preempt] [[advertising] interval *seconds*]
no vrrp *vrid vlan_id*
OmniSwitch 6450

vrrp *vrid vlan_id* address *ip_address*
vrrp *vrid vlan_id* no address *ip_address*
OmniSwitch 6450

vrrp track *track_id* [enable | disable] [priority *value*] [ipv4-interface *name* | ipv6-interface *name* |
port *slot*/*port* | address *address*]
no vrrp track *track_id*
OmniSwitch 6450

vrrp *vrid vlan_id* track-association *track_id*
vrrp *vrid vlan_id* no track-association *track_id*
OmniSwitch 6450

vrrp trap
no vrrp trap
OmniSwitch 6450

vrrp delay *seconds*
OmniSwitch 6450

vrrp interval *seconds*
OmniSwitch 6450

vrrp priority *priority*
OmniSwitch 6450

vrrp [preempt | no preempt]
OmniSwitch 6450

vrrp [disable | enable | enable all]
OmniSwitch 6450

vrrp set [interval | priority | preempt | all] [override]
OmniSwitch 6450

vrrp group *vrgid* **[interval** *seconds***] [priority** *priority***] [preempt | no preempt]**
no vrrp group *vrgid*
OmniSwitch 6450

vrrp group *vrgid* **[disable | enable | enable all]**

OmniSwitch 6450

vrrp group *vrgid* **set [interval | priority | preempt | all] [override]**
OmniSwitch 6450

vrrp *vrid vlan_id* **group-association** *vrgid*
vrrp *vrid vlan_id* **no group-association** *vrgid*
OmniSwitch 6450

vrrp3 *vrid vlan_id* [enable | disable | on | off] [priority *priority*] [preempt | no preempt][accept | no accept] [[advertising] interval *centiseconds*]
no vrrp3 *vrid vlan_id*
OmniSwitch 6450

vrrp3 *vrid vlan_id* address *ipv6_address*
vrrp3 *vrid vlan_id* no address *ipv6_address*
OmniSwitch 6450

vrrp3 trap
no vrrp3 trap
OmniSwitch 6450

vrrp3 *vrid vlan_id* track-association *track_id*
vrrp3 *vrid vlan_id* no track-association *track_id*
OmniSwitch 6450

show vrrp [*vrid*]
OmniSwitch 6450

show vrrp [*vrid*] statistics
OmniSwitch 6450

show vrrp track [*track_id*]
OmniSwitch 6450

show vrrp [*vrid*] track-association [*track_id*]
OmniSwitch 6450

show vrrp group [*vrgid***]**
OmniSwitch 6450

show vrrp group-association [*vrgid***]**
OmniSwitch 6450

show vrrp3 [*vrid*]
OmniSwitch 6450

show vrrp3 [*vrid*] statistics
OmniSwitch 6450

show vrrp3 [*vrid*] track-association [*track_id*]
OmniSwitch 6450

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]
OmniSwitch 6350, 6450

port mirroring *port_mirror_sessionid* {enable | disable}
no port mirroring *port_mirror_sessionid* {enable | disable}
OmniSwitch 6450, 6350

port monitoring *port_monitor_sessionid* source *slot/port*
[{no file | file *filename* [size *filesize*] | [overwrite {on | off}]}]
[inport | outport | bidirectional] [timeout *seconds*] [enable | disable]
OmniSwitch 6450, 6350

port monitoring *port_monitor_sessionid* {disable | pause | resume}
no port monitoring *port_monitor_sessionid*
OmniSwitch 6450, 6350

show port mirroring status [*port_mirror_sessionid*]
OmniSwitch 6450, 6350

show port monitoring status [*port_monitor_sessionid*]
OmniSwitch 6450, 6350

show port monitoring file [*port_monitor_sessionid*]
OmniSwitch 6450, 6350

Health Monitoring Commands

health threshold {rx *percent* | txrx *percent* | memory *percent* | cpu *percent* | temperature *degrees*}
OmniSwitch 6450, 6350

health threshold port-trap {*slot* | *slot/port* | *slot/port1-port2*} {**enable | disable**}
OmniSwitch 6450, 6350

health interval *seconds*
OmniSwitch 6450, 6350

health statistics reset
OmniSwitch 6450, 6350

show health threshold [rx | txrx | memory | cpu | temperature]
OmniSwitch 6450, 6350

show health threshold port-trap {*slot* | *slot/port* | *slot/port1-port2*}
OmniSwitch 6450, 6350

show health interval
OmniSwitch 6450, 6350

show health [*slot/port*] [statistics]
OmniSwitch 6450, 6350

show health all {memory | cpu | rx | txrx}
OmniSwitch 6450, 6350

show health slice *slot*
OmniSwitch 6450, 6350

sFlow Commands

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*
OmniSwitch 6450, 6350

sflow sampler num *portlist receiver receiver_index rate value sample-hdr-size size*
no sflow sampler num portlist
OmniSwitch 6450, 6350

sflow poller num portlist *receiver receiver_index interval value*
no sflow poller *num portlist*
OmniSwitch 6450, 6350

show sflow agent
OmniSwitch 6450, 6350

show sflow receiver [num]
OmniSwitch 6450, 6350

show sflow sampler[*num*]
OmniSwitch 6450, 6350

show sflow poller [*num*]
OmniSwitch 6450, 6350

QoS Commands

qos {enable | disable}
OmniSwitch 6450, 6350

qos trust ports
qos no trust ports

OmniSwitch 6450, 6350

qos default servicing mode {strict-priority | wrr [*w0 w1 w2 w3 w4 w5 w6 w7*] | drr] [*w0 w1 w2 w3 w4 w5 w6 w7*]}
OmniSwitch 6450, 6350

qos forward log
qos no forward log
OmniSwitch 6450, 6350

qos log console
qos no log console
OmniSwitch 6450, 6350

qos log lines *lines*
OmniSwitch 6450, 6350

qos log level *level*
qos no log level
OmniSwitch 6450, 6350

qos default bridged disposition {accept | deny | drop}
OmniSwitch 6450, 6350

qos default multicast disposition {accept | deny | drop}
OmniSwitch 6450, 6350

qos stats interval *seconds*
OmniSwitch 6450, 6350

qos nms priority
qos no nms priority
OmniSwitch 6450, 6350

qos phones {trusted | priority *priority_value}*
qos no phones
OmniSwitch 6450, 6350

qos user-port {filter | shutdown} {spoof | bpdu | rip | dhcp-server | dns-reply}
qos no user-port {filter | shutdown}
OmniSwitch 6450, 6350

qos dei egress
qos no dei egress
OmniSwitch 6450, 6350

qos force-yellow-priority *priority_value*
qos no force-yellow-priority
OmniSwitch 6450, 6350

qos force-yellow-802.1p *num*
qos no force-yellow-802.1p
OmniSwitch 6450, 6350

qos force-yellow-dscp *num*
qos no force-yellow-dscp
OmniSwitch 6450, 6350

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]
OmniSwitch 6450, 6350

debug qos internal [slice *slot/slice*] [flow] [queue] [port] [l2tree] [l3tree] [vector] [pending] [verbose] [mapper] [pool] [log] [pingonly | nopingonly]
OmniSwitch 6450, 6350

qos clear log
OmniSwitch 6450, 6350

qos apply
OmniSwitch 6450, 6350

qos revert
OmniSwitch 6450, 6350

qos flush
OmniSwitch 6450, 6350

qos reset
OmniSwitch 6450, 6350

qos stats reset [egress]
OmniSwitch 6450, 6350

qos port *slot/port* reset
OmniSwitch 6450, 6350

qos port *slot/port*
OmniSwitch 6450, 6350

qos port *slot/port* trusted
qos port *slot/port* no trusted
OmniSwitch 6450, 6350

qos port *slot/port* servicing mode {strict-priority | wrr [*w0 w1 w2 w3 w4 w5 w6 w7*] | drr [*w0 w1 w2 w3 w4 w5 w6 w7*] | default}
OmniSwitch 6450, 6350

qos port *slot/port* **q***n* **maxbw** *kbps*
qos port *slot/port* no **q***n* **maxbw** *kbps*
OmniSwitch 6450, 6350

qos port *slot/port* maximum egress-bandwidth *bps*
qos port *slot/port* no maximum egress-bandwidth
OmniSwitch 6450, 6350

qos port *slot/port* maximum ingress-bandwidth *bps*
qos port *slot/port* no maximum ingress-bandwidth
OmniSwitch 6450, 6350

qos port *slot/port* default 802.1p *value*
OmniSwitch 6450, 6350

qos port *slot/port* default dscp *value*
OmniSwitch 6450, 6350

qos port *slot/port* default classification {802.1p | dscp}
OmniSwitch 6450, 6350

qos port *slot/port* dei [egress]
qos port *slot/port* no dei [egress]
OmniSwitch 6450, 6350

show qos port [*slot/port*] [statistics]
OmniSwitch 6450, 6350

show qos queue [*slot/port*]
OmniSwitch 6450, 6350

show qos queue statistics [*slot/port*]
OmniSwitch 6450

show qos slice [*slot*/*slice*]
OmniSwitch 6450, 6350

show qos log
OmniSwitch 6450, 6350

show qos config
OmniSwitch 6450, 6350

show qos statistics
OmniSwitch 6450, 6350

qos register shared buffers <*num*>
OmniSwitch 6450, 6350

qos port[*slot/port*] register profile <*num*>

OmniSwitch 6450, 6350

show qos register
OmniSwitch 6450, 6350

QoS Policy Commands

policy rule *rule_name* [enable | disable] [precedence *precedence*] [condition *condition*] [action *action*] [validity period *name* | no validity period] [save] [accounting | no accounting] [log [interval *seconds*]] [count {packets | bytes}] [trap | no trap]
no policy rule *rule_name*
policy rule *rule_name* [no reflexive] [no save] [no log]
OmniSwitch 6450, 6350

policy rule *rule_name* accounting
policy rule *rule_name* no accounting
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

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*]...]
OmniSwitch 6450, 6350

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*...]
OmniSwitch 6450, 6350

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*]...]
OmniSwitch 6450, 6350

policy port group *group_name* [mode {split | non-split}] *slot/port*[-*port*] [*slot/port*[-*port*]...]
no policy port group *group_name*
policy port group *group_name* no *slot/port*[-*port*] [*slot/port*[-*port*]...]
OmniSwitch 6450, 6350

policy vlan group *group_name vlanstart*[-*vlanend*] [*vlanstart2*[-*vlanend2*]...]
no policy vlan group *group_name*
policy vlan group *group_name* no *vlanstart*[-*vlanend*] [*vlanstart2*[-*vlanend2*]...]
OmniSwitch 6450, 6350

policy map group *map_group* {*value1*:*value2*...}
no policy map group *map_group*
policy map group no {*value1*:*value2*...}
OmniSwitch 6450, 6350

policy service *service_name*
no policy service *service_name*
OmniSwitch 6450, 6350

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]
OmniSwitch 6450, 6350

policy service *service_name* source tcp port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no source tcp port
OmniSwitch 6450, 6350

policy service *service_name* destination tcp port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no destination tcp port
OmniSwitch 6450, 6350

policy service *service_name* source udp port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no source udp port
OmniSwitch 6450, 6350

policy service *service_name* destination udp port *port*[-*port*]
no policy service *service_name*
policy service *service_name* no destination udp port
OmniSwitch 6450, 6350

policy condition *condition_name*
no policy condition *condition_name*
OmniSwitch 6450, 6350

policy condition *condition_name* source ip *ip_address* [mask *netmask*]
policy condition *condition_name* no source ip
OmniSwitch 6450, 6350

policy condition *condition_name* source ipv6 {any | *ipv6_address* [mask *netmask*]}
policy condition *condition_name* no source ipv6
OmniSwitch 6450, 6350

policy condition *condition_name* destination ip *ip_address* [mask *netmask*]
policy condition *condition_name* no destination ip
OmniSwitch 6450, 6350

policy condition *condition_name* destination ipv6 {any | *ipv6_address* [mask *netmask*]}
policy condition *condition_name* no destination ipv6
OmniSwitch 6450, 6350

policy condition *condition_name* multicast ip *ip_address* [mask *netmask*]
policy condition *condition_name* no multicast ip
OmniSwitch 6450, 6350

policy condition *condition_name* source network group *network_group*
policy condition *condition_name* no source network group
OmniSwitch 6450, 6350

policy condition *condition_name* destination network group *network_group*
policy condition *condition_name* no destination network group
OmniSwitch 6450, 6350

policy condition *condition_name* multicast network group *multicast_group*
policy condition *condition_name* no multicast network group
OmniSwitch 6450, 6350

policy condition *condition_name* source ip port *port*[-*port*]
policy condition *condition_name* no source ip port
OmniSwitch 6450, 6350

policy condition *condition_name* destination ip port *port*[-*port*]
policy condition *condition_name* no destination ip port
OmniSwitch 6450, 6350

policy condition *condition_name* source tcp port *port*[-*port*]
policy condition *condition_name* no source tcp port
OmniSwitch 6450, 6350

policy condition *condition_name* destination tcp port *port*[-*port*]
policy condition *condition_name* no destination tcp port
OmniSwitch 6450, 6350

policy condition *condition_name* source udp port *port*[-*port*]
policy condition *condition_name* no source udp port
OmniSwitch 6450, 6350

policy condition *condition_name* destination udp port *port*[-*port*]
policy condition *condition_name* no destination udp port
OmniSwitch 6450, 6350

policy condition *condition_name* ethertype *etype*
policy condition *condition_name* no ethertype
OmniSwitch 6450, 6350

policy condition *condition_name* established
policy condition *condition_name* no established
OmniSwitch 6450, 6350

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
OmniSwitch 6450, 6350

policy condition *condition_name* service *service_name*
policy condition *condition_name* no service
OmniSwitch 6450, 6350

policy condition *condition_name* service group *service_group*
policy condition *condition_name* no service group
OmniSwitch 6450, 6350

policy condition *condition_name* icmptype *type*
policy condition *condition_name* no icmptype
OmniSwitch 6450, 6350

policy condition *condition_name* icmpcode *code*
policy condition *condition_name* no icmpcode
OmniSwitch 6450, 6350

policy condition *condition_name* ip protocol *protocol*
policy condition *condition_name* no ip protocol
OmniSwitch 6450, 6350

policy condition *condition_name* ipv6
policy condition *condition_name* no ipv6
OmniSwitch 6450, 6350

policy condition *condition_name* tos *tos_value* [mask *tos_mask*]
policy condition *conditioning* no tos
OmniSwitch 6450, 6350

policy condition *condition_name* dscp {*dscp_value*[-*value*]} [mask *dscp_mask*]
policy condition *condition_name* no dscp
OmniSwitch 6450, 6350

policy condition *condition_name* source mac *mac_address* [mask *mac_mask*]
policy condition *condition_name* no source mac
OmniSwitch 6450, 6350

policy condition *condition_name* destination mac *mac_address* [mask *mac_mask*]
policy condition *condition_name* no destination mac
OmniSwitch 6450, 6350

policy condition *condition_name* source mac group *group_name*
policy condition *condition_name* no source mac group
OmniSwitch 6450, 6350

policy condition *condition_name* destination mac group *mac_group*
policy condition *condition_name* no destination
OmniSwitch 6450, 6350

policy condition *condition_name* source vlan *vlan_id*
policy condition *condition_name* no source vlan
OmniSwitch 6450, 6350

policy condition *condition_name* source vlan group *vlan_group*
policy condition *condition_name* no source vlan group
OmniSwitch 6450, 6350

policy condition *condition_name* destination vlan *vlan_id*
policy condition *condition_name* no destination vlan
OmniSwitch 6450, 6350

policy condition *condition_name* 802.1p *802.1p*[-*802.1p_end*]

policy condition *condition_name* no 802.1p
OmniSwitch 6450, 6350

policy condition *condition_name* source port *slot/port*[*-port*]
policy condition *condition_name* no source port
OmniSwitch 6450, 6350

policy condition *condition_name* destination port *slot/port*[*-port*]
policy condition *condition_name* no destination port
OmniSwitch 6450, 6350

policy condition *condition_name* source port group *group_name*
policy condition *condition_name* no source port group
OmniSwitch 6450, 6350

policy condition *condition_name* destination port group *group_name*
policy condition *condition_name* no destination port
OmniSwitch 6450, 6350

policy action *action_name*
policy no action *action_name*
OmniSwitch 6450, 6350

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*...]
OmniSwitch 6450, 6350

policy action *action_name* disposition {accept | drop | deny}
policy action *action_name* no disposition
OmniSwitch 6450, 6350

policy action *action_name* shared
policy action *action_name* no shared
OmniSwitch 6450, 6350

policy action *action_name* priority *priority_value*
policy action *action_name* no priority
OmniSwitch 6450, 6350

policy action *action_name* maximum bandwidth *bps*
policy action *action_name* no maximum bandwidth
OmniSwitch 6450, 6350

policy action *action_name* maximum depth *bytes*
policy action *action_name* no maximum depth
OmniSwitch 6450, 6350

policy action action_name cir bps [cbs **byte**] [pir bps] [pbs **byte**]
policy action action_name no cir bps
OmniSwitch 6450, 6350

policy action *action_name* tos *tos_value*
policy action *action_name* no tos
OmniSwitch 6450, 6350

policy action *action_name* 802.1p *802.1p_value*
policy action *action_name* no 802.1p
OmniSwitch 6450, 6350

policy action *action_name* dscp *dscp_value*
policy action *action_name* no dscp
OmniSwitch 6450, 6350

policy action map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group*
policy action no map
OmniSwitch 6450, 6350

policy action *action_name* permanent gateway ip *ip_address*
policy action *action_name* no permanent gateway ip
OmniSwitch 6450, 6350

policy action *action_name* port-disable
policy action *action_name* no port-disable

OmniSwitch 6450, 6350

policy action *action_name* redirect port *slot/port*
policy action *action_name* no redirect port
OmniSwitch 6450, 6350

policy action *action_name* redirect linkagg *link_agg*
policy action *action_name* no redirect linkagg
OmniSwitch 6450, 6350

policy action *action_name* no-cache
policy action *action_name* no no-cache
OmniSwitch 6450, 6350

policy action *action_name* ingress mirror *slot/port*
policy action *action_name* no mirror *slot/port*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied]
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] source port *slot/port*
OmniSwitch 6450, 6350

OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] source mac *mac_address*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 multicast} [applied] destination mac *mac_address*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] source vlan *vlan_id*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] destination vlan *vlan_id*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] source interface type {ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] destination interface type {**ethernet | wan | ethernet-10 | ethernet-100 | ethernet-1G | ethernet-10G}**
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] 802.1p *value*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] source ip *ip_address*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] destination ip *ip_address*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] multicast ip *ip_address*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] tos *tos_value*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] dscp *dscp_value*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] ip protocol *protocol*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] source ip port *port*
OmniSwitch 6450, 6350

show policy classify {l2 | l3 | multicast} [applied] destination ip port *port*
OmniSwitch 6450, 6350

show [applied] policy network group [*network_group*]
OmniSwitch 6450, 6350

show [applied] policy service [*service_name*]
OmniSwitch 6450, 6350

show [applied] policy service group [*service_group*]
OmniSwitch 6450, 6350

show [applied] policy mac group [*mac_group*]
OmniSwitch 6450, 6350

show [applied] policy port group [*group_name*]
OmniSwitch 6450, 6350

show [applied] policy vlan group [*group_name*]
OmniSwitch 6450, 6350

show [applied] policy map group [*group_name*]
OmniSwitch 6450, 6350

show [applied] policy action [*action_name*]
OmniSwitch 6450, 6350

show [applied] policy list [*list_name*]
OmniSwitch 6450, 6350

show [applied] policy condition [*condition_name*]
OmniSwitch 6450, 6350

show active policy list [*list_name*]
OmniSwitch 6450, 6350

show active [bridged | routed | multicast] policy rule [*rule_name*] [extended]
OmniSwitch 6450, 6350

show active policy rule [*rule_name*] accounting
OmniSwitch 6450, 6350

show active policy list [*list_name*] accounting [details]
OmniSwitch 6450, 6350

show active policy rule [*rule_name*] meter-statistics [extended]
OmniSwitch 6450, 6350

show [applied] [bridged | routed | multicast] policy rule [*rule_name*]
OmniSwitch 6450, 6350

show policy validity period [*name*]
OmniSwitch 6450, 6350

policy action *action_name* {source | destination} rewrite ip *ip_address* [mask *netmask*]
policy action *action_name no* {source | destination} rewrite ip *ip_address* [mask *netmask*]
OmniSwitch 6450

qos nat timeout timeout_value
OmniSwitch 6450

show qos nat flows [protocol {UDP | TCP | ICMP} | outbound-ip ip_address | inbound {public-ip ip_address | private-ip ip_address]
OmniSwitch 6450

show qos nat counters
OmniSwitch 6450

qos nat flush
OmniSwitch 6450

Policy Server Commands

policy server load
OmniSwitch 6450, 6350

policy server flush
OmniSwitch 6450, 6350

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*]
OmniSwitch 6450, 6350

show policy server
OmniSwitch 6450, 6350

show policy server long
OmniSwitch 6450, 6350

show policy server statistics
OmniSwitch 6450, 6350

show policy server rules
OmniSwitch 6450, 6350

show policy server events
OmniSwitch 6450, 6350

IP Multicast Switching Commands

ip multicast [vlan *vid*] status [{enable | disable}]
OmniSwitch 6450, 6350

ip multicast flood-unknown {enable | disable}
OmniSwitch 6450, 6350

ip multicast dynamic-control drop-all status [{enable | disable}]
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] querier-forwarding [{enable | disable}]
no ip multicast [vlan *vid*] querier-forwarding
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] version [*version*]
OmniSwitch 6450, 6350

ip multicast max-group [num] [action {none | drop | replace}]
OmniSwitch 6450, 6350

ip multicast vlan vid max-group [num] [action {none | drop | replace}]
OmniSwitch 6450, 6350

ip multicast port slot | port max-group [num] [action {none | drop | replace}]
OmniSwitch 6450, 6350

ip multicast static-neighbor vlan *vid* port *slot*/*port*
no ip multicast static-neighbor vlan *vid* port *slot*/*port*
OmniSwitch 6450, 6350

ip multicast static-neighbor fast-convergence {enable | disable}
OmniSwitch 6450, 6350

ip multicast static-querier vlan *vid* port *slot*/*port*
no ip multicast static-querier vlan *vid* port *slot*/*port*
OmniSwitch 6450, 6350

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>]*
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] query-interval [*seconds*]
OmniSwitch 6450, 6350

ip multicast [vlan vid**]** last-member-query-interval [tenths-of-seconds**]**
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] query-response-interval [*tenths-of-seconds*]
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] unsolicited-report-interval [*seconds*]
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] router-timeout [*seconds*]
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] source-timeout [*seconds*]
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] querying [{enable | disable}]
no ip multicast [vlan *vid*] querying
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] robustness [*robustness*]
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] spoofing [{enable | disable}]
no ip multicast [vlan *vid*] spoofing
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] zapping [{enable | disable}]
OmniSwitch 6450, 6350

ip multicast [vlan *vid*] proxying [enable | disable]
OmniSwitch 6450, 6350

ip multicast star-g-mode status {enable | disable}
ip multicast vlan *vlan-id* star-g-mode status {enable | disable}
ipv6 multicast [vlan *vid*] status [{enable | disable}]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] querier-forwarding [{enable | disable}]
no ipv6 multicast [vlan *vid*] querier-forwarding
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] version [*version*]
OmniSwitch 6450, 6350

ipv6 multicast max-group [num] [action {none | drop | replace}]
OmniSwitch 6450, 6350

ipv6 multicast vlan vid max-group [num] [action {none | drop | replace}]
OmniSwitch 6450, 6350

ipv6 multicast port slot | port max-group [num] [action {none | drop | replace}]
OmniSwitch 6450, 6350

ipv6 multicast static-neighbor vlan *vid* port *slot*/*port*
no ipv6 multicast static-neighbor vlan *vid* port *slot*/*port*
OmniSwitch 6450, 6350

ipv6 multicast static-querier vlan *vid* port *slot*/*port*
no ipv6 multicast static-querier vlan *vid* port *slot*/*port*
OmniSwitch 6450, 6350

ipv6 multicast static-group *ip_address* vlan *vid* port *slot*/*port*
no ipv6 multicast static-group *ip_address* vlan *vid* port *slot*/*port*
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] query-interval [*seconds*]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] last-member-query-interval [*milliseconds*]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] query-response-interval [*milliseconds*]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] unsolicited-report-interval [*seconds*]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] router-timeout [*seconds*]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] source-timeout [*seconds*]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] querying [{enable | disable}]

no ipv6 multicast [vlan *vid*] querying
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] robustness [*robustness*]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] spoofing [{enable | disable}]
no ipv6 multicast [vlan *vid*] spoofing
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] zapping [{enable | disable}]
OmniSwitch 6450, 6350

ipv6 multicast [vlan *vid*] proxying [enable | disable]
OmniSwitch 6450, 6350

show ip multicast [vlan *vid*]
OmniSwitch 6450, 6350

show ip multicast port [slot/*port*]
OmniSwitch 6450, 6350

show ip multicast forward [*ip_address*]
OmniSwitch 6450, 6350

show ip multicast neighbor
OmniSwitch 6450, 6350

show ip multicast querier
OmniSwitch 6450, 6350

show ip multicast group [*ip_address*]
OmniSwitch 6450, 6350

show ip multicast source [*ip_address*]
OmniSwitch 6450, 6350

show ipv6 multicast [vlan *vid*]
OmniSwitch 6450, 6350

show ipv6 multicast port [slot/*port*]
OmniSwitch 6450, 6350

show ipv6 multicast forward [*ipv6_ddress*]
OmniSwitch 6450, 6350

show ipv6 multicast neighbor
OmniSwitch 6450, 6350

show ipv6 multicast querier
OmniSwitch 6450, 6350

show ipv6 multicast group [*ip_address*]
OmniSwitch 6450, 6350

show ipv6 multicast source [*ip_address*]
OmniSwitch 6450, 6350

IP Multicast VLAN Commands

vlan ipmvlan *ipmvlan-id* [{enable | disable} | [{1x1 | flat} stp {enable | disable}]] [name *name-string*] [svlan]
no vlan ipmvlan *ipmvlan-id* [-*ipmvlan-id2*]
OmniSwitch 6450, 6350

vlan ipmvlan *ipmvlan-id* ctag {*ctag* | *ctag1-ctag2*}
no vlan ipmvlan *ipmvlan-id* ctag {*ctag* | *ctag1-ctag2*}
OmniSwitch 6450

vlan ipmvlan *ipmvlan-id* address {*ip_address* | *ipv6_address* | *ipaddress1-ipaddress2* | *ipv6address1-ipv6address2*}
no vlan ipmvlan *ipmvlan-id* address {*ip_address* | *ipv6_address* | *ipaddress1-ipaddress2* | *ipv6address1-ipv6address2*}
OmniSwitch 6450, 6350

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***]**}
OmniSwitch 6450, 6350

vlan ipmvlan *ipmvlan-id* receiver-port {port slot/port[-*port2***]** | linkagg *agg_num* **[**-*agg_num2***]**}
[*receiver vlan-id***]**
no vlan ipmvlan *ipmvlan-id* receiver-port {port slot/port**[**-*port2***]** | linkagg *agg_num* **[**-*agg_num2***]**}
[*receiver vlan-id***]**
OmniSwitch 6450, 6350

vlan svlan port **{**slot/port | *agg_num***}** *translate cvlan customer-vlan-id {*ipmvlan *ipmvlan-id* | *svlan svlan-id***}**
vlan svlan port **{**slot/port | *agg_num***}** *cvlan customer-vlan-id no* ipmvlan *ipmvlan-id*
OmniSwitch 6450

show vlan ipmvlan [*ipmvlan-id*] c-tag
OmniSwitch 6450

show vlan ipmvlan [*ipmvlan-id***] address**
OmniSwitch 6450, 6350

show vlan ipmvlan [*ipmvlan-id***] port-config**
OmniSwitch 6450, 6350

show vlan ipmvlan port-config [slot/port | agg_num]
OmniSwitch 6450, 6350

show vlan ipmvlan port-binding [*slot/port* | *agg_num*]
OmniSwitch 6450, 6350

AAA Commands

aaa radius-server *server* host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*] {key *secret* | hash-key *hash_secret*|| prompt-key} [salt *salt* | hash-salt *hash_salt*] [retransmit *retries*] [timeout *seconds*] [auth-port *auth_port*] [acct-port *acct_port*] [mac-address-format-status {enable | disable} mac-address-format {uppercase | lowercase}] [nas-port {default | ifindex} | nas-port-id {enable | disable}] nas-port-type [xdsl | x75x25 | x25 | wireless-other | wireless-ieee-802-11 | virtual | sync | sdsl-symmetric-dsl | piafs | isdn-sync | isdn-async-v120 | isdn-async-v110 | idsl | hdlc-clear-channel | g3-fax | Ethernet | cable | async | adsl-dmt | adsl-cap-asymmetric-dsl] [unique-acct-session-id {enable | disable}]
no aaa radius server *server*
OmniSwitch 6450, 6350

aaa test-radius-server *server-name* type {authentication user *user-name* password *password* [method {MD5 | PAP}] | accounting user *user-name*}
OmniSwitch 6450, 6350

aaa radius-health-check name *server-name* status {enable | disable} polling-interval *seconds* username *user-name* password *password* failover {enable | disable}
no aaa radius-health-check name server-name
OmniSwitch 6450

aaa tacacs+-server *server* host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*] [key *secret* || hash-key *hash_secret*|| prompt-key] [salt *salt* | hash-salt *hash_salt*] [timeout *seconds*] [port *port*]
no aaa tacacs+-server *server*
OmniSwitch 6450, 6350

aaa tacacs command-authorization {enable | disable}
OmniSwitch 6450, 6350

aaa tacacs server-wait-time *num*
OmniSwitch 6450, 6350

aaa ldap-server *server_name* host {*hostname* | *ip_address*} [{*hostname2* | *ip_address2}*] dn *dn_name* {password *super_password* | *hash-password hash_super_password* | *prompt-password}* [salt *salt* | hash-salt *hash_salt*] base *search_base* [retransmit *retries*] [timeout *seconds*] [ssl | no ssl] [port *port*]
no aaa ldap-server *server-name*
OmniSwitch 6450, 6350

aaa ace-server clear
OmniSwitch 6450, 6350

aaa authentication {console | telnet | ftp | http | snmp | ssh | default} { local |default | ACE} *server1* [*server2*...]
no aaa authentication {console | telnet | ftp | http | snmp | ssh | default}
OmniSwitch 6450, 6350

aaa authentication {console | telnet | ftp | http | snmp | ssh} default
OmniSwitch 6450, 6350

aaa authentication 802.1x *server1* [*server2*] [*server3*] [*server4*] [*server5*]
no aaa authentication 802.1x
OmniSwitch 6450, 6350

aaa authentication MAC *server1* [*server2*] [*server3*] [*server4*] [*server5*]
no aaa authentication MAC
OmniSwitch 6450, 6350

aaa accounting 802.1x *server1* [*server2*...] [local]
no aaa accounting 802.1x
OmniSwitch 6450, 6350

aaa accounting mac *server1* [*server2*...] [local]
no aaa accounting mac
OmniSwitch 6450, 6350

aaa accounting session *server1* [*server2*...] [local]
no accounting session
OmniSwitch 6450, 6350

aaa accounting command *server1* [*server2*...] [local]
no accounting command
OmniSwitch 6450, 6350

user *username* {password *password* | password-prompt} [expiration {*day* | *date*}] [read-only | read-write [*families...* | *domains...*| view *viewname* | all | none | all-except *families...*]] [no snmp | no auth | sha | md5 | sha+des | md5+des | sha+3des | sha+aes | sha+aes192 | sha+aes256 | sha224 | sha224+3des | sha224+aes | sha224+aes192 | sha224+aes256 | sha256 | sha256+3des | sha256+aes | sha256+aes192 | sha256+aes256]] [priv-password *password* | prompt-priv-passwd] [console-only {enable | disable}]
no user *username*
OmniSwitch 6450, 6350

password
OmniSwitch 6450, 6350

user password-size min *size*
OmniSwitch 6450, 6350

user password-expiration {*day* | disable}
OmniSwitch 6450, 6350

user password-policy cannot-contain-username {enable | disable}
OmniSwitch 6450, 6350

user password-policy min-uppercase *number*
OmniSwitch 6450, 6350

user password-policy min-lowercase *number*
OmniSwitch 6450, 6350

user password-policy min-digit *number*
OmniSwitch 6450, 6350

user password-policy min-nonalpha *number*
OmniSwitch 6450, 6350

user password-history *number*
OmniSwitch 6450, 6350

user password-min-age *days*
OmniSwitch 6450, 6350

user lockout-window *minutes*
OmniSwitch 6450, 6350

user lockout-threshold *number*
OmniSwitch 6450, 6350

user lockout-duration *minutes*
OmniSwitch 6450, 6350

user *profile* {lockout | unlock}
OmniSwitch 6450, 6350

aaa admin-logout {mac-address *mac_address* | port *slot/port* | user *user_name* | user-network-profile name *profile_name*}
OmniSwitch 6450, 6350

system common-criteria admin-state {enable | disable}
OmniSwitch 6450, 6350

show system common-criteria
OmniSwitch 6450, 6350

aaa certificate update-ca-certificate ca_file
OmniSwitch 6450, 6350

aaa certificate update-crl crl_file
OmniSwitch 6450, 6350

aaa certificate generate-rsa-key key-file key_file
OmniSwitch 6450, 6350

aaa certificate generate-self-signed key-file {key_file} [days valid_period} {CN common_name} {ON org_name} {OU org_unit} {L locality} {ST state} {C country}
OmniSwitch 6450, 6350

aaa certificate view cert_file
OmniSwitch 6450, 6350

aaa certificate delete cert_file
OmniSwitch 6450, 6350

aaa certificate generate-csr key-file {key_file}{CN common_name} {ON org_name} {OU org_unit} {L locality} {ST state} {C country}
OmniSwitch 6450, 6350

end-user profile *name* [read-only [*area* | all]] [read-write [*area* | all]] [disable [*area* | all]]
no end-user profile *name*
OmniSwitch 6450, 6350

OmniSwitch 6450, 6350

end-user profile *name* vlan-range *vlan_range* [*vlan_range2...*]
end-user profile *name* no vlan-range *vlan1* [*vlan2..*]
OmniSwitch 6450, 6350

aaa user-network-profile name *profile_name* vlan *vlan-id* [hic {enable | disable}] [redirect url_name] [policy-list-name *list_name*] [maximum-ingress-bandwidth num [K(kilo) | M(mega)| G (giga)| T (tera)]] [maximum-egress-bandwidth num [K(kilo) | M(mega)| G (giga)| T (tera)]] [maximum-default-depth num [K(kilo) | M(mega)| G (giga)| T (tera)]]
no aaa user-network-profile name *name*
OmniSwitch 6450, 6350

aaa classification-rule mac-address *mac_address* user-network-profile name *profile_name*
aaa classification-rule no mac-address *mac_address*
OmniSwitch 6450, 6350

aaa radius nas-identifier { user-string *text_string* | default }
OmniSwitch 6450, 6350

aaa radius nas-ip-address {default | local-ip [*ip_address*] }
OmniSwitch 6450, 6350

show aaa radius config
OmniSwitch 6450, 6350

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*
OmniSwitch 6450, 6350

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*]
OmniSwitch 6450, 6350

aaa classification-rule lldp med-endpoint access-point user-network-profile name *profile_name*
OmniSwitch 6450, 6350

[no] aaa byod white-list *ip_address* [*subnet_mask*]
OmniSwitch 6450, 6350

aaa byod white-list no *ip_address*
OmniSwitch 6450, 6350

aaa hic server-name *server* ip-address *ip_address {***key** *key* | prompt-key} [role {primary | backup}] [udp-port *udp_port*]
aaa hic no server-name *server*
OmniSwitch 6450, 6350

aaa hic allowed-name *server* ip-address *ip_address* **[mask** *subnet_mask*]
aaa hic no allowed-name *server*
OmniSwitch 6450, 6350

aaa hic {enable | disable}
OmniSwitch 6450, 6350

aaa hic web-agent-url *url*
OmniSwitch 6450, 6350

aaa hic custom-proxy-port *proxy_port*
OmniSwitch 6450, 6350

aaa hic redundancy background-poll-interval value
OmniSwitch 6450, 6350

aaa hic server-failure mode {hold | passthrough}
OmniSwitch 6450, 6350

aaa hic server-failure policy user-network-profile change unp1 to unp2
aaa hic server-failure policy user-network-profile no change
OmniSwitch 6450, 6350

show aaa server [*server_name*]
OmniSwitch 6450, 6350

show aaa radius-health-check config
OmniSwitch 6450

show radius-server [server name] statistics
OmniSwitch 6450, 6350

clear radius-server [server_name] statistics
OmniSwitch 6450, 6350

show aaa authentication
OmniSwitch 6450, 6350

show aaa authentication 802.1x
OmniSwitch 6450, 6350

show aaa authentication mac

OmniSwitch 6450, 6350

show aaa authentication 802.1x
OmniSwitch 6450, 6350

show aaa authentication mac [statistics]
OmniSwitch 6450, 6350

show aaa accounting
OmniSwitch 6450, 6350

show user [*username*]
OmniSwitch 6450, 6350

show user password-size
OmniSwitch 6450, 6350

show user password-expiration
OmniSwitch 6450, 6350

show user password-policy
OmniSwitch 6450, 6350

show user lockout-setting
OmniSwitch 6450, 6350

debug command-info {enable | disable}
OmniSwitch 6450, 6350

debug end-user profile *name*
OmniSwitch 6450, 6350

show end-user profile *name*
OmniSwitch 6450, 6350

show aaa user-network-profile
OmniSwitch 6450, 6350

show aaa classification-rule {mac-rule | mac-range-rule | ip-net-rule | lldp-rule}
OmniSwitch 6450, 6350

show aaa hic
OmniSwitch 6450, 6350

show aaa hic host
OmniSwitch 6450, 6350

show aaa hic server
OmniSwitch 6450, 6350

show aaa hic allowed
OmniSwitch 6450, 6350

show aaa hic server-failure policy
OmniSwitch 6450, 6350

show aaa-device all-users [unp *profile_name* | policy *device_policy* | authentication-status [success | fail]] [port *slot/port*]
OmniSwitch 6450, 6350

show aaa-device supplicant-users [unp *profile_name* | policy *device_policy* | authentication-status [success | fail]] [port *slot/port*]
OmniSwitch 6450, 6350

show aaa-device non-supplicant-users [unp *profile_name* | policy *device_policy* | authentication-status [success | fail]] [port *slot/port*]
OmniSwitch 6450, 6350

show aaa-device captive-portal-users [unp *profile_name* | policy *device_policy* | authentication-status [success | fail]] [port *slot/port*]
OmniSwitch 6450

show aaa priv hexa [*domain or family*]
OmniSwitch 6450, 6350

aaa redirect-server name hostname hostname ip-address ip_address url-list {redirect_url1 redirect_url2 redirect_url3}
OmniSwitch 6450, 6350

aaa redirect *name* url {*url_name*}
OmniSwitch 6450, 6350

aaa port-bounce [slot/port | slot | slot/port1-portn] {enable | disable}
OmniSwitch 6450, 6350

aaa redirect pause-timer seconds
OmniSwitch 6450, 6350

aaa redirect proxy-server-port *proxy_port*
no aaa rediret proxy-server-port
OmniSwitch 6450, 6350

show aaa redirect-server
OmniSwitch 6450, 6350

show aaa redirect url-list
OmniSwitch 6450, 6350

show aaa port-bounce status slot/port
OmniSwitch 6450, 6350

show aaa redirect pause-timer
OmniSwitch 6450, 6350

show byod host
OmniSwitch 6450, 6350

show byod status slot/port
OmniSwitch 6450, 6350

show aaa byod white-list ip address
OmniSwitch 6450, 6350

show aaa user-network-profile
OmniSwitch 6450, 6350

mdns-relay {enable | disable}
OmniSwitch 6450

mdns-relay tunnel ip interface name
no mdns-relay tunnel ip interface name
OmniSwitch 6450

zeroconf mdns admin-state {enable | disable}
OmniSwitch 6450

zeroconf ssdp admin-state {enable | disable}
OmniSwitch 6450

zeroconf mode [gateway] [tunnel [type standard]]
OmniSwitch 6450

zeroconf responder-ip ipv4address
no zeroconf responder-ip ipv4address
OmniSwitch 6450

zeroconf gateway-vlan-list vlan-id1...vlan-idn
no zeroconf gateway-vlan-list vlan-id1...vlan-idn
OmniSwitch 6450

zeroconf access-vlan-list vlan-id1...vlan-idn
no zeroconf access-vlan-list vlan-id1...vlan-idn
OmniSwitch 6450

show mdns-relay config
OmniSwitch 6450

show zeroconf config
OmniSwitch 6450

aaa switch-access mode {default | enhanced}

OmniSwitch 6450, 6350

aaa switch-access ip-lockout-threshold number
OmniSwitch 6450, 6350

aaa switch-access banned-ip {all | ip_address} release
OmniSwitch 6450, 6350

aaa switch-access priv-mask {console | telnet | ssh | http | https} {read-only | read-write} [*families...* | *domains...*| all | none | all-except *families...*]
OmniSwitch 6450, 6350

aaa switch-access management-stations {enable | disable}
OmniSwitch 6450, 6350

aaa switch-access management-stations ip_address [**mask** *mask*]
no aaa switch-access management-stations ip_address
OmniSwitch 6450, 6350

show aaa switch-access mode
OmniSwitch 6450, 6350

show aaa switch-access ip-lockout-threshold
OmniSwitch 6450, 6350

show aaa switch-access banned-ip
OmniSwitch 6450, 6350

show aaa switch-access priv-mask
OmniSwitch 6450, 6350

show aaa switch-access management-stations
OmniSwitch 6450, 6350

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]
OmniSwitch 6450, 6350

802.1x initialize *slot/port*
OmniSwitch 6450, 6350

802.1x reauthenticate *slot/port*
OmniSwitch 6450, 6350

802.1x *slot/port* **supp-polling retry** *retries*
OmniSwitch 6450, 6350

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 | mac-authentication}...]
OmniSwitch 6450, 6350

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}]
OmniSwitch 6450, 6350

802.1x **captive-portal name** *cp_url_name*
802.1x captive-portal no name
OmniSwitch 6450

802.1x *slot/port* **non-supplicant policy {**group-mobility | user-network-profile profile_name | vlan *vid* | default-vlan | block | captive-portal}
OmniSwitch 6450, 6350

802.1x *slot/port* **{supplicant | non-supplicant} policy default**

OmniSwitch 6450, 6350

802.1x *slot/port* **captive-portal policy authentication pass {group-mobility | user-network-profile profile_name | vlan** *vid* | default-vlan | block}] [fail] {group-mobility | **user-network-profile profile_name** vlan *vid* | default-vlan | block}
OmniSwitch 6450

802.1x *slot/port* **captive-portal session-limit** *time*
OmniSwitch 6450

802.1x *slot/port* **captive-portal inactivity-logout** *{enable | disable}*
OmniSwitch 6450

802.1x *slot/port* **captive-portal** retry-count *retries*
OmniSwitch 6450

802.1x **captive-portal** address *ip_address*
OmniSwitch 6450

802.1x **delay-learning num**
OmniSwitch 6450, 6350

802.1x **captive-portal** proxy-server-url *proxy_url*
OmniSwitch 6450

802.1x **captive-portal** proxy-server-port *proxy_port*
802.1x **captive-portal no** proxy-server-port *proxy_port*
OmniSwitch 6450

802.1x **captive-portal** dns-keyword-list {*keyword1* [*keyword2*] **[***keyword3***] [***keyword4***]}**
802.1x captive-portal no dns-keyword-list
OmniSwitch 6450

802.1x **captive-portal** success-redirect-url *redirect_url*
802.1x captive-portal no success-redirect-url
OmniSwitch 6450

802.1x **captive-portal** fail-redirect-url *redirect_url*
802.1x captive-portal no fail-redirect-url
OmniSwitch 6450

802.1x **auth-server-down {enable | disable}**
OmniSwitch 6450, 6350

802.1x **auth-server-down policy {user-network-profile** *profile_name* | **block}**
OmniSwitch 6450, 6350

802.1x **auth-server-down re-authperiod {value}**
OmniSwitch 6450, 6350

802.1x **auth-server-down {enable | disable}**
OmniSwitch 6450, 6350

802.1x **auth-server-down [[no] voice-policy] [policy] {user-network-profile** *profile_name* | **block}**
802.1x auth-server-down no voice-policy
OmniSwitch 6450, 6350

802.1x server-polling {enable | disable}
OmniSwitch 6450, 6350

802.1x *slot/port* trust-radius {enable | disable}
OmniSwitch 6450, 6350

802.1x *slot/port* non-supplicant session-timeout {enable | disable} [interval *num]* [trust-radius {enable | disable}] [inactivity-logout {enable | disable}]
OmniSwitch 6450, 6350

show 802.1x [*slot/port*]
OmniSwitch 6450, 6350

show 802.1x users [*slot/port*]
OmniSwitch 6450, 6350

show 802.1x ap-client-mac *slot/port*
OmniSwitch 6450, 6350

show 802.1x statistics [*slot/port*]
OmniSwitch 6450, 6350

show 802.1x device classification policies [*slot/port*]
OmniSwitch 6450, 6350

show 802.1x captive-portal configuration
OmniSwitch 6450

show 802.1x non-supplicant [*slot/port*]
OmniSwitch 6450, 6350

show 802.1x auth-server-down
OmniSwitch 6450, 6350

show 802.1x rate-limit [*slot/port*]
802.1x *slot/port* **supplicant bypass** {enable | disable}
OmniSwitch 6450, 6350

802.1x *slot/port* **non-supplicant allow-eap {pass | fail | noauth | none}**
OmniSwitch 6450, 6350

802.1x **pass-through {enable | disable}**
OmniSwitch 6450, 6350

show 802.1x captive-portal configuration [*slot/port*]
OmniSwitch 6450, 6350

Switch Logging Commands

swlog
no swlog
OmniSwitch 6450, 6350

swlog syslog-facility-id {*facility_id* | *integer*}
OmniSwitch 6450, 6350

swlog appid {*app_id* | *integer*} level {*level* | *integer*}
no swlog appid *app_id*
OmniSwitch 6450, 6350

swlog remote command-log {enable | disable}
OmniSwitch 6450, 6350

swlog output {console | flash | socket [*ip_address]*}
no swlog output {console | flash | socket *[ip_address]*}
OmniSwitch 6450, 6350

swlog output flash file-size *bytes*
OmniSwitch 6450, 6350

swlog clear
OmniSwitch 6450, 6350

show log swlog
show log swlog [session *session_id*] [timestamp *start_time* [*end_time*]] [appid *appid*] [level *level*]
OmniSwitch 6450, 6350

show swlog
OmniSwitch 6450, 6350

OmniVista Cirrus Commands

cloud-agent admin-state {enable | disable | disable force | restart}
OmniSwitch 6450, 6350

show cloud-agent status
OmniSwitch 6450, 6350

show cloud-agent vpn status
OmniSwitch 6450, 6350

Index

802.1ab 13-1
  notification of local system MIB changes 13-12
  reinit delay 13-8
  show port statistics 13-36
  tlv management 13-18
  transmit time interval 13-5
802.1p
  mapped to ToS or DSCP 45-141
  QoS port default 44-56
802.1Q 15-1
  show 15-5
  untrusted ports 44-5
802.1X 50-1
  device classification policy 50-19
  supplicant policy authentication 50-10, 50-67, 50-69, 50-71
  supp-polling retry 50-8

A

AAA 49-1
  password-size min 49-46
  show user network profile 49-141, 49-145, 49-147, 49-149, 49-151, 49-153, 49-155, 49-158, 49-161, 49-164
  show user password-expiration 49-130
Access-Node-Identifier 21-8
accounting 23-65, 23-99
actions
  supported by hardware 45-117
active login sessions 6-34
Alcatel Mapping Adjacency Protocol 14-1
  adjacent switches 14-2
  common transmission state 14-5
  discovery transmission state 14-3
alerts 51-6, 51-14
alias 6-17
AMAP
  see Alcatel Mapping Adjacency Protocol
ASA Configuration
  verify information about 6-10
assigning ports to VLANs 25-8
authenticated mobile ports 24-21, 24-23, 24-25, 24-26, 24-28
authenticated VLANs
  DHCP Relay 37-9

B

boot.cfg file
  QoS log lines 44-11
BPDU
  see Bridge Protocol Data Units
Bridge Protocol Data Units 16-4, 16-94, 16-96, 16-97, 16-99

C

CCM
  priority value 29-33
  transmission interval 29-15
  transmission rate 29-31
circuit-id
  ascii 21-10
  cvlan 21-10
  delimeter 21-10
CLI
  logging commands 6-29, 6-54–6-56
client 21-6
CMM
  reload 1-2
  running configuration 1-6
  show running-directory 1-6
  takeover 1-13
CMS 3-1
  allocated addresses 3-9
  display status 3-11
  MAC address release 3-6
  mac retention status 3-4
  mac-range 3-2
  range table 3-7
commands
  domains and families 49-42, 49-208
conditions
  multiple conditions defined 45-40
Continuity Check Messages
  see CCM
counters 23-101
current user session 6-32

D

Daylight Savings Time (DST)
  enabling or disabling 2-12
debug messages 51-6, 51-14
default route
  IP 34-17
DHCP Relay 37-1
  AVLAN only forwarding option 37-9
  DHCP server IP address 37-4
  dhcp snooping option-82 format 37-26, 37-28, 37-30
  elapsed boot time 37-13
  forward delay time 37-13
  Global DHCP 37-4
  ip helper pre-support 37-21
  maximum number of hops 37-15
  per-VLAN forwarding option 37-11
  show ip helper 37-78
  standard forwarding option 37-8
  statistics 37-83, 37-85
DHCP VLAN rules 24-2, 24-4, 24-6, 24-8
directory
  change 7-3

create 7-6
delete 7-8
display 7-5, 7-10, 7-28, 7-30, 7-34
rename 7-14
DNS
domain name 11-2
enables resolver 11-2
name servers 11-2, 11-3, 11-7, 11-9
resolver 11-1
DSCP
mapped to 802.1p or ToS 45-141
QoS port default 44-58
duplex data transfer 23-31
dynamic link aggregation
adding ports 12-22
creating 12-9
deleting 12-9
deleting ports 12-22
LACPDU frames 12-25, 12-31
local port MAC address 12-27
remote group MAC address 12-18
remote port MAC address 12-33
dynamic VLAN assignment
mobile ports 24-20
dynamic VLAN port assignment
secondary VLANs 24-24
VLAN rules 24-1

E

editor
vi 7-36
error file 9-4
error frame 23-71, 23-103
errors 51-6, 51-14
Ethernet 23-1
clear port violation 23-26, 23-43, 23-120
interfaces 23-6
trap port 23-4
ethernet domain 29-5, 29-57
Ethernet OAM 29-1
association endpoint list 29-17, 29-19
lowest priority fault alarm 29-27, 29-35, 29-37, 29-39
maintenance association 29-9
exit 6-31

F

fault alarm
alarm time 29-45
reset time 29-47
file
copy 7-18, 7-20, 7-32
delete 7-16, 7-31, 7-33
move 7-22
privileges 7-26
starting ftpv6 session 7-45
starting sftpv6 session 7-52
system check 7-28, 7-29
transfer 7-43, 7-45, 7-54

G

GARP 26-1
GVRP 26-1, 27-1
applicant 26-9, 27-11
disable 26-2, 27-2
disable on specified port 26-3, 27-4
display configuration on specified port 26-4, 26-8, 26-10, 26-12, 26-14, 26-16, 26-18, 26-26, 26-27, 26-28, 26-30, 27-33, 27-36, 27-49
enable 26-2, 27-2, 27-4, 34-10
enable on specified port 26-3, 26-27, 26-30, 27-4
registration 26-7, 27-10
timer 26-11, 27-13, 27-28

H

health 42-2

I

IGMP
default 47-11, 47-90, 47-93, 47-111
group entry 47-23, 47-96, 47-102, 47-104
ip multicast querier-forwarding 47-9
last member query interval 47-27, 47-90, 47-93, 47-111
neighbor entry 47-19, 47-97
querier entry 47-21, 47-99
query interval 47-25, 47-90, 47-93, 47-111
query response interval 47-29, 47-31, 47-90, 47-93, 47-111
querying 47-9, 47-37, 47-90, 47-93, 47-111
robustness variable 47-39, 47-90, 47-93, 47-111
router timeout 47-33, 47-90, 47-93, 47-111
source timeout 47-35, 47-90, 47-93, 47-111
spoofing 47-41, 47-90, 47-93, 47-111
zapping 47-43, 47-45, 47-90, 47-93, 47-111
inter-frame gap 23-18, 23-109, 23-113
Intermediate Agent 21-1
IP Multicast Switching
see IPMS 47-1
IP network address VLAN rule 24-14
IP routing
default route 34-17
IPMS 47-1
ipv6 multicast querier-forwarding 47-49
IPMV 48-1
assign ipv4, ipv6 address 48-6
association 48-12
create 48-2
customer VLAN ID 48-4
delete 48-2
ipv4, ipv6 address 48-15
receiver port 48-10
sender port 48-8
show ipmvlan port-config 48-19
ipv6
address 35-6
dad-check 35-8
hop-limit 35-9

host 35-11
interface 35-3
neighbor 35-12, 35-13
ping6 35-24
pmtu-lifetime 35-9, 35-10
prefix 35-15
rip 35-70
route 35-17, 35-18
traceroute 35-26

L

LACP
see dynamic link aggregation
line speed 23-33
Link Trace Messages 29-43
priority value 29-33
loopback messages 29-41
LPS 22-1
learn-trap-threshold 22-22
max-filtering 22-10
maximum 22-8
shutdown 22-4

M

MAC address table
duplicate MAC addresses 20-3
MAC address VLAN rule 24-10, 24-12, 49-87, 49-88, 49-89, 49-90, 49-91, 49-92, 49-93, 49-144
MAC addresses
aging time 16-41, 16-43, 16-45, 20-6
dynamic link aggregation 12-18, 12-27, 12-33
learned 20-2
statically assigned 20-2, 20-3, 20-5
Maintenance Association
create 29-9
modify 29-17
Maintenance Intermediate Point
see MIP
Management Domain
display all information 29-4, 29-6, 29-7, 29-8, 29-48, 29-54, 29-57, 30-4, 30-6, 30-8, 30-12, 30-14, 30-16, 30-18, 30-20, 30-21, 30-23, 30-32
display specific information 29-6, 29-7, 29-8, 29-56, 30-4, 30-6, 30-8, 30-12, 30-14, 30-16, 30-18
MEP 29-24
administrative state 29-17, 29-29
MHF value 29-7
MLD
default 47-51, 47-108
group entry 47-63, 47-113, 47-119, 47-121
last member query interval 47-67, 47-108
neighbor entry 47-59, 47-114
querier entry 47-61, 47-116
query interval 47-65, 47-108
query response interval 47-69, 47-71, 47-108
querying 47-77, 47-108
robustness variable 47-79, 47-108
router timeout 47-73, 47-108
source timeout 47-75, 47-108
spoofing 47-81, 47-108
zapping 47-83, 47-85, 47-108
mobile port properties
authentication 24-21, 24-23, 24-25, 24-26, 24-28
BPDU ignore 24-20, 24-21
default VLAN membership 24-24
restore default VLAN 24-22
status 24-32
mobile ports 24-20
VLAN rules 24-1
modules
power 2-22
reloading 2-18, 2-20
temperature 2-23, 2-30

N

Network Interface (NI) modules
reloading 2-14, 2-16, 2-17
NTP 5-1
broadcast delay 5-8
key 5-9
operation 5-6
server 5-2
server unsynchronization 5-5
synchronization 5-4

P

pending configuration
commands associated with 44-39
erasing policy configuration 44-39
PMM
port mirroring 41-2
port monitoring source 41-7
policies
save option 45-6
policy condition
dscp 45-90
source vlan 45-100, 45-102
policy servers
displaying information about 46-6
SSL 46-4
port mapping 33-2
port mobility
see mobile ports
port status 23-109
port VLAN rule 24-18
PPPoE Intermediate Agent 21-1
prompt 6-14
protocol VLAN rules 24-16

Q

QOS
ip phone traffic 44-20
nms priority 44-18

R

RDP
- advertisement packets 36-5
- maximum time 36-7, 36-11
- minimum time 36-9
- preference level 36-13

remote-id 21-13, 21-18
resolver
- *see* DNS resolver

Ring Rapid Spanning Tree Protocol
- create 16-111, 16-112, 16-116
- disable 16-111
- enable 16-111
- remove 16-112

RIP
- active peer 39-29
- forced hold-down timer 39-12
- garbage timer 39-20
- global 39-2
- hold-down timer 39-21
- host-route 39-14
- IGP 39-1
- interface 39-4
- invalid timer 39-19
- route-tag 39-15
- security 39-16
- status 39-3

RMON
- probes 38-2

router discovery protocol
- *see* RDP 36-1

S

secure shell session 6-46, 6-47, 6-48, 6-49, 7-51, 7-53
secure socket layer
- *see* SSL

session management
- banner 6-5
- history buffer 6-24
- kills 6-30
- login attempt 6-3
- more 6-41
- more size 6-40
- prompt 6-8
- timeout 6-7
- user profile 6-20, 6-21, 6-22
- xon-xoff 6-12, 6-13

sflow 43-5
- poller 43-7
- receiver 43-3
- sampler 43-5

smurf attack 34-27
snapshot 9-11
SNMP
- community map 10-8
- community strings 10-8
- security 10-12
- station 10-3
- statistics 10-16
- trap 10-20

source learning 20-1
- MAC address table 20-1, 20-2, 20-5

Spanning Tree Algorithm and Protocol 16-1
- 1x1 operating mode 16-4, 16-12, 16-14, 16-17, 16-19, 16-26, 16-28, 16-124
- bridge ID 16-21, 16-23, 16-25, 16-27
- flat operating mode 16-4, 16-12, 16-14, 16-17, 16-19, 16-26, 16-28, 16-124
- path cost 16-68, 16-72, 16-75, 16-79
- port ID 16-59, 16-61, 16-63, 16-65
- port states 16-81, 16-83, 16-85
- pvst+ mode 16-175
- rrstp ring vlan-tag 16-114

Spanning Tree bridge parameters
- maximum aging time 16-35

Spanning Tree port parameters
- connection type 16-87, 16-88, 16-89, 16-90, 16-91, 16-92, 16-94, 16-96, 16-97, 16-100, 16-101, 16-102, 16-103, 16-104, 16-105, 16-106, 16-107, 16-108
- link aggregate ports 16-53, 16-55, 16-57
- mode 16-81, 16-83, 16-85
- path cost 16-83, 16-85
- priority 16-59
- Spanning Tree status 16-53, 16-55, 16-57

ssh6 6-49
SSL 8-3
- policy servers 46-4

static link aggregation
- creating 12-3
- deleting 12-3

static MAC addresses 20-2, 20-3, 20-5
syntax check 9-9
system information
- administrative contact 2-3
- date 2-6
- location 2-5
- name 2-4
- time 2-6, 2-7
- time zone 2-9

T

telnet 6-43, 6-45
timer session 9-6
ToS
- mapped to 802.1p or DSCP 45-141
- QoS port default 44-58

trust 21-6

U

UDLD 32-1
- clear UDLD statistics 32-10
- probe-message advertisement timer 32-6
- show global status 32-12
- show neighbor ports 32-17

user accounts
- SNMP access 49-42

UTC 5-1

V

VLAN rules 24-1
DHCP 24-2, 24-4, 24-6, 24-8
IP network address 24-14
MAC address 24-10, 24-12, 49-87, 49-88, 49-89, 49-90, 49-91, 49-92, 49-93, 49-144
port 24-18
protocol 24-16
VLAN Stacking
display list of all or range of configured SVLANs 28-44, 28-45, 28-49, 28-50, 28-76
ethernet-service sap 28-18
ethernet-service uni-profile 28-29, 28-35, 28-37, 28-38, 28-40
show ethernet-service mode 28-44
VLANs 17-1, 25-1, 25-2
administrative status 25-2
default VLAN 25-8
description 25-2
operational status 25-2
port assignments 25-8
rules 24-1
secondary VLAN 25-8
Spanning Tree status 25-4
VRRP
configure address 40-5
configure/modify 40-3
configuring priority 40-4
delay 40-10
display configuration 40-35
display statistics 40-38
display track-association 40-43
display tracking policies 40-41
enable/disable trap 40-9
group 40-21
preempt 40-15
priority 40-13
set 40-19
show vrrp group-association 40-47
track-association 40-8
tracking policy 40-6
VRRP3
configure address 40-32
configure/modify 40-29
display configuration 40-49
display statistics 40-52
display track-association 40-54
enable/disable trap 40-33
track-association 40-34

W

warnings 51-6, 51-14
WebView
enabling/disabling 8-2

Z

Zmodem 7-56