

Part No. 060321-10, Rev. E
September 2012

OmniSwitch CLI Reference Guide

Alcatel-Lucent 

www.alcatel-lucent.com

**This user guide documents AOS Release 7 for the OmniSwitch 10K and OmniSwitch 6900.
The functionality described in this guide is subject to change without notice.**

Copyright © 2012 by Alcatel-Lucent. All rights reserved. This document may not be reproduced in whole or in part without the express written permission of Alcatel-Lucent.

Alcatel-Lucent® and the Alcatel-Lucent logo are registered trademarks of Alcatel-Lucent. Xylan®, OmniSwitch®, OmniStack®, and Alcatel-Lucent OmniVista® are registered trademarks of Alcatel-Lucent.

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

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

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



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

**US Customer Support—(800) 995-2696
International Customer Support—(818) 878-4507
Internet—service.esd.alcatel-lucent.com**

Contents

	About This Guide	xxix
	Supported Platforms	xxix
	Who Should Read this Manual?	xxix
	When Should I Read this Manual?	xxix
	What is in this Manual?	xxx
	What is Not in this Manual?	xxx
	How is the Information Organized?	xxx
	Text Conventions	xxxi
	Documentation Roadmap	xxxii
	Related Documentation	xxxiv
	Technical Support	xxxv
Chapter 1	Ethernet Port Commands	1-1
	interfaces	1-3
	interfaces speed	1-5
	interfaces crossover	1-7
	interfaces duplex	1-9
	interfaces alias	1-11
	clear interfaces l2-statistics	1-12
	interfaces max-frame-size	1-13
	interfaces flood-limit	1-14
	interfaces ingress-bandwidth	1-16
	interfaces pause	1-17
	interfaces link-trap	1-19
	interfaces ddm	1-20
	interfaces ddm-trap	1-21
	clear violation	1-22
	show interfaces	1-23
	show interfaces alias	1-27
	show interfaces status	1-29
	show interfaces capability	1-31
	show interfaces accounting	1-33
	show interfaces counters	1-36
	show interfaces counters errors	1-38
	show interfaces flood-rate	1-40
	show interfaces traffic	1-42
	show interfaces ingress-rate-limit	1-44
	show interfaces ddm	1-46
	show transceivers	1-49
	show violation	1-51

Chapter 2	UDLD Commands	2-1
	udld	2-2
	udld port	2-3
	udld mode	2-5
	udld probe-timer	2-7
	udld echo-wait-timer	2-9
	clear udld statistics port	2-11
	show udld configuration	2-12
	show udld configuration port	2-14
	show udld statistics port	2-16
	show udld neighbor port	2-18
	show udld status port	2-20
Chapter 3	Source Learning Commands	3-1
	mac-learning	3-2
	mac-learning flush	3-4
	mac-learning flush domain	3-5
	mac-learning static mac-address	3-7
	mac-learning multicast mac-address	3-9
	mac-learning aging-time	3-11
	mac-learning mode	3-13
	show mac-learning	3-14
	show mac-learning remote	3-17
	show mac-learning aging-time	3-19
	show mac-learning learning-state	3-20
	show mac-learning mode	3-22
	mac-ping	3-23
Chapter 4	VLAN Management Commands	4-1
	vlan	4-2
	vlan members untagged	4-4
	vlan members tagged	4-6
	vlan mtu-ip	4-8
	show vlan	4-10
	show vlan members	4-13
Chapter 5	High Availability VLAN Commands	5-1
	server-cluster	5-2
	server-cluster vlan	5-4
	server-cluster mac-address	5-6
	server-cluster ip	5-8
	server-cluster igmp mode	5-10
	server-cluster ip-multicast	5-12
	server-cluster port	5-14
	server-cluster linkagg	5-16
	show server-cluster	5-18
Chapter 6	Distributed Spanning Tree Commands	6-1
	spantree mode	6-3
	spantree protocol	6-5
	spantree vlan admin-state	6-7
	spantree mst region name	6-8

spantree mst region revision-level	6-10
spantree mst region max-hops	6-11
spantree msti	6-13
spantree msti vlan	6-15
spantree priority	6-17
spantree hello-time	6-20
spantree max-age	6-22
spantree forward-delay	6-24
spantree bpdu-switching	6-26
spantree path-cost-mode	6-28
spantree pvst+compatibility	6-30
spantree auto-vlan-containment	6-32
spantree cist	6-34
spantree vlan	6-36
spantree cist path-cost	6-38
spantree msti path-cost	6-41
spantree vlan path-cost	6-44
spantree cist mode	6-47
spantree vlan mode	6-49
spantree cist connection	6-51
spantree vlan connection	6-53
spantree cist admin-edge	6-55
spantree vlan admin-edge	6-57
spantree cist auto-edge	6-59
spantree vlan auto-edge	6-61
spantree cist restricted-role	6-63
spantree vlan restricted-role	6-65
spantree cist restricted-tcn	6-67
spantree vlan restricted-tcn	6-69
spantree cist txholdcount	6-71
spantree vlan txholdcount	6-72
show spantree	6-73
show spantree cist	6-76
show spantree msti	6-80
show spantree vlan	6-85
show spantree ports	6-89
show spantree cist ports	6-92
show spantree msti ports	6-96
show spantree vlan ports	6-102
show spantree mode	6-108
show spantree mst	6-110
show spantree msti vlan-map	6-112
show spantree cist vlan-map	6-114
show spantree map-msti	6-116

Chapter 7	Shortest Path Bridging Commands	7-1
	spb bvlan	7-3
	spb isis bvlan ect-id	7-5
	spb isis control-bvlan	7-6
	spb isis bvlan tandem-multicast-mode	7-7
	spb isis bridge-priority	7-9
	spb isis interface	7-10

spb isis admin-state	7-12
spb isis area-address	7-13
spb isis source-id	7-14
spb isis spf-wait	7-15
spb isis lsp-wait	7-17
spb isis overload	7-19
spb isis overload-on-boot	7-21
spb isis graceful-restart	7-23
spb isis graceful-restart helper	7-24
show spb isis info	7-25
show spb isis bvlans	7-28
show spb isis interface	7-30
show spb isis adjacency	7-32
show spb isis database	7-35
show spb isis nodes	7-38
show spb isis unicast-table	7-40
show spb isis services	7-42
show spb isis spf	7-44
show spb isis multicast-table	7-46
show spb isis multicast-sources	7-48
show spb isis multicast-sources-spf	7-50
show spb isis ingress-mac-filter	7-52
Chapter 8	
Link Aggregation Commands	8-1
linkagg static agg size	8-3
linkagg static agg name	8-6
linkagg static agg admin-state	8-8
linkagg static port agg	8-9
linkagg lacp agg size	8-11
linkagg lacp agg name	8-14
linkagg lacp agg admin-state	8-16
linkagg lacp agg actor admin-key	8-18
linkagg lacp agg actor system-priority	8-19
linkagg lacp agg actor system-id	8-21
linkagg lacp agg partner system-id	8-23
linkagg lacp agg partner system-priority	8-25
linkagg lacp agg partner admin-key	8-27
linkagg lacp port actor admin-key	8-29
linkagg lacp port actor admin-state	8-32
linkagg lacp port actor system-id	8-34
linkagg lacp port actor system-priority	8-36
linkagg lacp agg partner admin-state	8-38
linkagg lacp port partner admin system-id	8-40
linkagg lacp port partner admin-key	8-42
linkagg lacp port partner admin system-priority	8-44
linkagg lacp port actor port priority	8-46
linkagg lacp port partner admin-port	8-48
linkagg lacp port partner admin port-priority	8-50
linkagg range	8-52
show linkagg	8-54
show linkagg port	8-59
show linkagg range	8-65

Chapter 9	Multi-Chassis Commands	9-1
	multi-chassis chassis-id	9-2
	multi-chassis hello-interval	9-4
	multi-chassis ipc-vlan	9-6
	multi-chassis chassis-group	9-8
	multi-chassis loop-detection	9-10
	multi-chassis loop-detection transmit-interval	9-12
	multi-chassis vf-link create	9-14
	multi-chassis vf-link member-port	9-16
	multi-chassis vf-link default-vlan	9-18
	multi-chassis vip-vlan	9-20
	show multi-chassis status	9-22
	show multi-chassis loop-detection	9-24
	show multi-chassis vf-link	9-26
	show multi-chassis vf-link member-port	9-28
	show multi-chassis consistency	9-30
	show multi-chassis consistency linkagg	9-33
	clear multi-chassis loop-detection	9-36
Chapter 10	Ethernet Ring Protection Commands	10-1
	erp-ring	10-2
	erp-ring rpl-node	10-5
	erp-ring wait-to-restore	10-7
	erp-ring enable	10-8
	erp-ring guard-timer	10-9
	erp-ring sub-ring	10-10
	erp-ring virtual-channel	10-13
	erp-ring revertive	10-15
	erp-ring clear	10-17
	erp-ring ethoam-event	10-18
	clear erp statistics	10-20
	show erp	10-22
	show erp statistics	10-25
Chapter 11	MVRP Commands	11-1
	mvrp	11-2
	mvrp port	11-3
	mvrp linkagg	11-5
	mvrp maximum-vlan	11-7
	mvrp registration	11-8
	mvrp applicant	11-10
	mvrp timer join	11-12
	mvrp timer leave	11-14
	mvrp timer leaveall	11-16
	mvrp timer periodic-timer	11-18
	mvrp periodic-transmission	11-20
	mvrp restrict-vlan-registration	11-21
	mvrp restrict-vlan-advertisement	11-23
	mvrp static-vlan-restrict	11-25
	show mvrp configuration	11-27
	show mvrp port	11-28
	show mvrp linkagg	11-31

	show mvrp timer	11-33
	show mvrp statistics	11-36
	show mvrp last-pdu-origin	11-39
	show mvrp vlan-restrictions	11-41
	mvrp clear-statistics	11-43
Chapter 12	802.1AB Commands	12-1
	lldp transmit interval	12-2
	lldp transmit hold-multiplier	12-3
	lldp transmit delay	12-4
	lldp reinit delay	12-5
	lldp notification interval	12-6
	lldp lldpdu	12-7
	lldp notification	12-9
	lldp tlv management	12-11
	lldp tlv dot1	12-13
	lldp tlv dot3	12-15
	lldp tlv med	12-17
	show lldp system-statistics	12-19
	show lldp statistics	12-21
	show lldp local-system	12-23
	show lldp local-port	12-25
	show lldp local-management-address	12-30
	show lldp remote-system	12-31
	show lldp config	12-33
	show lldp statistics	12-35
	show lldp remote-system med	12-37
Chapter 13	IP Commands	13-1
	ip interface	13-5
	ip interface tunnel	13-8
	ip router primary-address	13-10
	ip router router-id	13-11
	ip static-route	13-12
	ip route-pref	13-14
	ip default-ttl	13-16
	ping	13-17
	traceroute	13-19
	ip directed-broadcast	13-21
	ip service	13-22
	ip service port	13-24
	ip redistrib	13-26
	ip access-list	13-28
	ip access-list address	13-29
	ip route-map action	13-31
	ip route-map match ip address	13-33
	ip route-map match ipv6 address	13-35
	ip route-map match ip-nexthop	13-37
	ip route-map match ipv6-nexthop	13-39
	ip route-map match tag	13-41
	ip route-map match ipv4-interface	13-43
	ip route-map match ipv6-interface	13-45

ip route-map match metric	13-47
ip route-map match route-type	13-49
ip route-map match protocol	13-51
ip route-map set metric	13-53
ip route-map set metric-type	13-55
ip route-map set tag	13-57
ip route-map set community	13-59
ip route-map set local-preference	13-61
ip route-map set level	13-63
ip route-map set ip-nexthop	13-65
ip route-map set ipv6-nexthop	13-67
vrf	13-69
ip export route-map	13-71
ip import vrf	13-73
show ip export	13-75
show ip import	13-76
show ip global-route-table	13-77
arp	13-79
clear arp-cache	13-81
ip dos arp-poison restricted-address	13-82
arp filter	13-83
clear arp filter	13-85
icmp type	13-86
icmp unreachable	13-88
icmp echo	13-90
icmp timestamp	13-92
icmp addr-mask	13-94
icmp messages	13-96
ip dos scan close-port-penalty	13-97
ip dos scan tcp open-port-penalty	13-98
ip dos scan udp open-port-penalty	13-99
ip dos scan threshold	13-100
ip dos trap	13-102
ip dos scan decay	13-103
show ip traffic	13-104
show ip interface	13-107
show ip routes	13-112
show ip route-pref	13-114
show ip redistrib	13-116
show ip access-list	13-118
show ip route-map	13-120
show ip router database	13-122
show ip emp-routes	13-125
show ip config	13-127
show ip protocols	13-128
show ip router-id	13-130
show ip service	13-131
show ip dos arp-poison	13-133
show arp	13-134
show arp filter	13-136
show icmp control	13-138
show icmp statistics	13-140

	show tcp statistics	13-142
	show tcp ports	13-144
	show udp statistics	13-146
	show udp ports	13-147
	show ip dos config	13-148
	show ip dos statistics	13-150
	show vrf	13-152
Chapter 14	IPv6 Commands	14-1
	ipv6 interface	14-3
	ipv6 interface tunnel source destination	14-7
	ipv6 address	14-8
	ipv6 address global-id	14-10
	ipv6 address local-unicast	14-11
	ipv6 dad-check	14-13
	ipv6 hop-limit	14-14
	ipv6 pmtu-lifetime	14-15
	ipv6 neighbor stale-lifetime	14-16
	ipv6 neighbor	14-17
	ipv6 prefix	14-19
	ipv6 static-route	14-21
	ipv6 route-pref	14-23
	ipv6 virtual-source-mac	14-25
	ping6	14-26
	traceroute6	14-28
	show ipv6 icmp statistics	14-30
	show ipv6 interface	14-33
	show ipv6 pmtu table	14-37
	show ipv6 neighbors	14-38
	clear ipv6 neighbors	14-40
	show ipv6 prefixes	14-41
	show ipv6 routes	14-43
	show ipv6 route-pref	14-45
	show ipv6 router database	14-46
	show ipv6 tcp connections	14-48
	show ipv6 tcp listeners	14-50
	show ipv6 traffic	14-52
	show ipv6 tunnel configured	14-55
	show ipv6 tunnel 6to4	14-57
	show ipv6 udp ports	14-58
	show ipv6 information	14-60
	ipv6 redistrib	14-62
	ipv6 access-list	14-64
	ipv6 access-list address	14-65
	show ipv6 redistrib	14-67
	show ipv6 access-list	14-69
	ipv6 load rip	14-71
	ipv6 rip admin-state	14-72
	ipv6 rip invalid-timer	14-73
	ipv6 rip garbage-timer	14-74
	ipv6 rip holddown-timer	14-75
	ipv6 rip jitter	14-76

	ipv6 rip route-tag	14-77
	ipv6 rip update-interval	14-78
	ipv6 rip triggered-sends	14-79
	ipv6 rip interface	14-80
	ipv6 rip interface metric	14-82
	ipv6 rip interface recv-status	14-83
	ipv6 rip interface send-status	14-84
	ipv6 rip interface horizon	14-85
	show ipv6 rip	14-86
	show ipv6 rip interface	14-88
	show ipv6 rip peer	14-91
	show ipv6 rip routes	14-93
Chapter 15	IPsec commands	15-1
	ipsec key	15-2
	ipsec security-key	15-4
	ipsec policy	15-6
	ipsec policy rule	15-9
	ipsec sa	15-11
	show ipsec policy	15-13
	show ipsec sa	15-15
	show ipsec key	15-17
	show ipsec ipv6 statistics	15-19
Chapter 16	RIP Commands	16-1
	ip load rip	16-2
	ip rip admin-state	16-3
	ip rip interface	16-4
	ip rip interface admin-state	16-6
	ip rip interface metric	16-8
	ip rip interface send-version	16-9
	ip rip interface recv-version	16-11
	ip rip interface ingress-filter	16-13
	ip rip interface ingress-filter	16-14
	ip rip interface egress-filter	16-15
	ip rip force-holddowntimer	16-16
	ip rip host-route	16-18
	ip rip route-tag	16-19
	ip rip interface auth-type	16-20
	ip rip interface auth-key	16-21
	ip rip update-interval	16-22
	ip rip invalid-timer	16-23
	ip rip garbage-timer	16-24
	ip rip holddown-timer	16-25
	show ip rip	16-26
	show ip rip routes	16-28
	show ip rip interface	16-31
	show ip rip peer	16-33
Chapter 17	BFD Commands	17-1
	ip bfd admin-state	17-3
	ip bfd transmit	17-4

ip bfd receive	17-5
ip bfd multiplier	17-6
ip bfd echo-interval	17-7
ip bfd interface	17-8
ip bfd interface admin-state	17-9
ip bfd interface transmit	17-10
ip bfd interface receive	17-11
ip bfd interface multiplier	17-12
ip bfd interface echo-interval	17-13
ip ospf bfd-state	17-14
ip ospf bfd-state all-interfaces	17-16
ip ospf interface bfd-state	17-17
ip ospf interface bfd-state drs-only	17-18
ip ospf interface bfd-state all-neighbors	17-19
ip bgp bfd-state	17-20
ip bgp bfd-state all-neighbors	17-21
ip bgp neighbor bfd-state	17-22
vrrp bfd-state	17-23
vrrp track address bfd-state	17-24
show ip bfd	17-25
show ip bfd interfaces	17-27
show ip bfd sessions	17-29
show ip bfd sessions statistics	17-31
ip static-route all bfd-state	17-33
ip static-route bfd-state	17-34
Chapter 18	
DHCP Relay Commands	18-1
ip helper address	18-2
ip helper vlan address	18-4
ip helper standard	18-6
ip helper per-vlan-only	18-7
ip helper forward-delay	18-9
ip helper maximum-hops	18-11
ip helper agent-information	18-13
ip helper agent-information policy	18-15
ip helper pxe-support	18-17
ip helper boot-up	18-18
ip helper boot-up enable	18-19
ip udp relay port	18-20
ip udp relay service	18-22
ip udp relay service vlan	18-24
show ip helper	18-26
show ip helper statistics	18-28
show ip udp relay	18-30
show ip udp relay statistics	18-32
no ip helper statistics	18-34
ip udp relay no statistics	18-36
Chapter 19	
VRRP Commands	19-1
vrrp	19-3
vrrp address	19-5
vrrp track	19-6

vrrp track-association	19-8
vrrp trap	19-9
vrrp delay	19-10
vrrp interval	19-11
vrrp priority	19-13
vrrp preempt	19-15
vrrp all	19-17
vrrp set	19-19
vrrp group	19-21
vrrp group all	19-23
vrrp group set	19-25
vrrp group-association	19-27
vrrp3	19-29
vrrp3 address	19-32
vrrp3 trap	19-33
vrrp3 track-association	19-34
show vrrp	19-35
show vrrp statistics	19-38
show vrrp track	19-41
show vrrp track-association	19-43
show vrrp group	19-45
show vrrp group-association	19-47
show vrrp3	19-49
show vrrp3 statistics	19-52
show vrrp3 track-association	19-54

Chapter 20

OSPF Commands	20-1
ip ospf admin-state	20-3
ip load ospf	20-4
ip ospf asbr	20-5
ip ospf exit-overflow-interval	20-6
ip ospf extlsdb-limit	20-7
ip ospf host	20-8
ip ospf mtu-checking	20-10
ip ospf default-originate	20-11
ip ospf route-tag	20-13
ip ospf spf-timer	20-14
ip ospf virtual-link	20-16
ip ospf neighbor	20-19
ip ospf area	20-21
ip ospf area default-metric	20-23
ip ospf area range	20-25
ip ospf interface	20-27
ip ospf interface admin-state	20-28
ip ospf interface area	20-29
ip ospf interface auth-key	20-30
ip ospf interface auth-type	20-31
ip ospf interface dead-interval	20-33
ip ospf interface hello-interval	20-34
ip ospf interface md5	20-35
ip ospf interface md5 key	20-37
ip ospf interface type	20-39

ip ospf interface cost	20-41
ip ospf interface poll-interval	20-42
ip ospf interface priority	20-43
ip ospf interface retrans-interval	20-44
ip ospf interface transit-delay	20-45
ip ospf restart-support	20-46
ip ospf restart-interval	20-47
ip ospf restart-helper admin-state	20-48
ip ospf restart-helper strict-lsa-checking admin-state	20-49
ip ospf restart initiate	20-51
show ip ospf	20-52
show ip ospf border-routers	20-55
show ip ospf ext-lsdb	20-57
show ip ospf host	20-59
show ip ospf lsdb	20-61
show ip ospf neighbor	20-63
show ip ospf routes	20-66
show ip ospf virtual-link	20-68
show ip ospf virtual-neighbor	20-70
show ip ospf area	20-73
show ip ospf area range	20-76
show ip ospf area stub	20-78
show ip ospf interface	20-80
show ip ospf restart	20-86
Chapter 21	
OSPFv3 Commands	21-1
ipv6 ospf admin-state	21-3
ipv6 load ospf	21-4
ipv6 ospf host	21-5
ipv6 ospf mtu-checking	21-7
ipv6 ospf route-tag	21-8
ipv6 ospf spf-timer	21-9
ipv6 ospf virtual-link	21-11
ipv6 ospf area	21-13
ipv6 ospf interface	21-15
ipv6 ospf interface admin-state	21-16
ipv6 ospf interface area	21-17
ipv6 ospf interface dead-interval	21-18
ipv6 ospf interface hello-interval	21-20
ipv6 ospf interface cost	21-21
ipv6 ospf interface priority	21-22
ipv6 ospf interface retrans-interval	21-23
ipv6 ospf interface transit-delay	21-24
show ipv6 ospf	21-25
show ipv6 ospf border-routers	21-28
show ipv6 ospf host	21-30
show ipv6 ospf lsdb	21-32
show ipv6 ospf neighbor	21-34
show ipv6 ospf routes	21-36
show ipv6 ospf virtual-link	21-38
show ipv6 ospf area	21-40
show ipv6 ospf interface	21-42

Chapter 22	BGP Commands	22-1
	ip load bgp	22-6
	ip bgp admin-state	22-7
	ip bgp autonomous-system	22-8
	ip bgp bestpath as-path ignore	22-9
	ip bgp cluster-id	22-11
	ip bgp default local-preference	22-13
	ip bgp fast-external-failover	22-15
	ip bgp always-compare-med	22-17
	ip bgp bestpath med missing-as-worst	22-18
	ip bgp client-to-client reflection	22-19
	ip bgp as-origin-interval	22-21
	ip bgp synchronization	22-22
	ip bgp confederation identifier	22-24
	ip bgp maximum-paths	22-26
	ip bgp log-neighbor-changes	22-27
	ip bgp dampening	22-28
	ip bgp dampening clear	22-31
	ip bgp aggregate-address	22-32
	ip bgp aggregate-address admin-state	22-34
	ip bgp aggregate-address as-set	22-36
	ip bgp aggregate-address community	22-38
	ip bgp aggregate-address local-preference	22-40
	ip bgp aggregate-address metric	22-42
	ip bgp aggregate-address summary-only	22-44
	ip bgp network	22-46
	ip bgp network admin-state	22-48
	ip bgp network community	22-50
	ip bgp network local-preference	22-51
	ip bgp network metric	22-53
	ip bgp neighbor	22-55
	ip bgp neighbor admin-state	22-56
	ip bgp neighbor advertisement-interval	22-57
	ip bgp neighbor clear	22-58
	ip bgp neighbor route-reflector-client	22-60
	ip bgp neighbor default-originate	22-61
	ip bgp neighbor timers	22-62
	ip bgp neighbor conn-retry-interval	22-64
	ip bgp neighbor auto-restart	22-66
	ip bgp neighbor maximum-prefix	22-68
	ip bgp neighbor md5 key	22-70
	ip bgp neighbor ebgp-multihop	22-72
	ip bgp neighbor description	22-74
	ip bgp neighbor next-hop-self	22-75
	ip bgp neighbor passive	22-77
	ip bgp neighbor remote-as	22-78
	ip bgp neighbor remove-private-as	22-80
	ip bgp neighbor soft-reconfiguration	22-81
	ip bgp neighbor stats-clear	22-83
	ip bgp confederation neighbor	22-84
	ip bgp neighbor update-source	22-85
	ip bgp neighbor in-aspathlist	22-87

ip bgp neighbor in-communitylist	22-88
ip bgp neighbor in-prefixlist	22-89
ip bgp neighbor out-aspathlist	22-90
ip bgp neighbor out-communitylist	22-91
ip bgp neighbor out-prefixlist	22-92
ip bgp neighbor route-map	22-93
ip bgp neighbor clear soft	22-95
ip bgp policy aspath-list	22-96
ip bgp policy aspath-list action	22-99
ip bgp policy aspath-list priority	22-101
ip bgp policy community-list	22-103
ip bgp policy community-list action	22-105
ip bgp policy community-list match-type	22-107
ip bgp policy community-list priority	22-109
ip bgp policy prefix-list	22-111
ip bgp policy prefix-list action	22-113
ip bgp policy prefix-list ge	22-114
ip bgp policy prefix-list le	22-116
ip bgp policy prefix6-list	22-118
ip bgp policy route-map	22-120
ip bgp policy route-map action	22-122
ip bgp policy route-map aspath-list	22-123
ip bgp policy route-map asprepend	22-124
ip bgp policy route-map community	22-125
ip bgp policy route-map community-list	22-127
ip bgp policy route-map community-mode	22-128
ip bgp policy route-map lpref	22-130
ip bgp policy route-map lpref-mode	22-131
ip bgp policy route-map match-community	22-133
ip bgp policy route-map match-mask	22-135
ip bgp policy route-map match-prefix	22-136
ip bgp policy route-map match-regexp	22-137
ip bgp policy route-map med	22-139
ip bgp policy route-map med-mode	22-140
ip bgp policy route-map origin	22-142
ip bgp policy route-map prefix-list	22-144
ip bgp policy route-map weight	22-146
ip bgp policy route-map community-strip	22-147
show ip bgp	22-148
show ip bgp statistics	22-151
show ip bgp dampening	22-153
show ip bgp dampening-stats	22-155
show ip bgp path	22-157
show ip bgp routes	22-161
show ip bgp aggregate-address	22-163
show ip bgp network	22-165
show ip bgp neighbors	22-167
show ip bgp neighbors policy	22-172
show ip bgp neighbors timer	22-174
show ip bgp neighbors statistics	22-176
show ip bgp policy aspath-list	22-181
show ip bgp policy community-list	22-183

show ip bgp policy prefix-list	22-185
show ip bgp policy route-map	22-187
ip bgp graceful-restart	22-190
ip bgp graceful-restart restart-interval	22-191
ip bgp unicast	22-192
ipv6 bgp unicast	22-193
ip bgp neighbor activate-ipv6	22-194
ip bgp neighbor ipv6-next-hop	22-195
show ipv6 bgp path	22-196
show ipv6 bgp routes	22-200
ipv6 bgp network	22-202
ipv6 bgp network community	22-203
ipv6 bgp network local-preference	22-205
ipv6 bgp network metric	22-207
ipv6 bgp network admin-state	22-209
show ipv6 bgp network	22-210
ipv6 bgp neighbor	22-212
ipv6 bgp neighbor activate-ipv6	22-214
ipv6 bgp neighbor ipv6-next-hop	22-215
ipv6 bgp neighbor admin-state	22-216
ipv6 bgp neighbor remote-as	22-217
ipv6 bgp neighbor timers	22-218
ipv6 bgp neighbor maximum-prefix	22-220
ipv6 bgp neighbor next-hop-self	22-222
ipv6 bgp neighbor conn-retry-interval	22-223
ipv6 bgp neighbor default-originate	22-224
ipv6 bgp neighbor update-source	22-225
ipv6 bgp neighbor ipv4-next-hop	22-226
show ipv6 bgp neighbors	22-227
show ipv6 bgp neighbors statistics	22-232
show ipv6 bgp neighbors policy	22-237
show ipv6 bgp neighbors timers	22-239

Chapter 23	Server Load Balancing Commands	23-1
	ip slb admin-state	23-2
	ip slb reset statistics	23-3
	ip slb cluster	23-4
	ip slb cluster admin-state	23-6
	ip slb cluster ping period	23-7
	ip slb cluster ping timeout	23-9
	ip slb cluster ping retries	23-11
	ip slb cluster probe	23-12
	ip slb server ip cluster	23-13
	ip slb server ip cluster probe	23-15
	ip slb probe	23-16
	ip slb probe timeout	23-18
	ip slb probe period	23-20
	ip slb probe port	23-22
	ip slb probe retries	23-24
	ip slb probe username	23-26
	ip slb probe password	23-27
	ip slb probe url	23-28

ip slb probe status	23-29
ip slb probe send	23-30
ip slb probe expect	23-31
show ip slb	23-32
show ip slb clusters	23-34
show ip slb cluster	23-37
show ip slb cluster server	23-41
show ip slb servers	23-44
show ip slb probes	23-46
Chapter 24	
IP Multicast Switching Commands	24-1
ip multicast admin-state	24-3
ip multicast querier-forwarding	24-5
ip multicast version	24-7
ip multicast max-group	24-9
ip multicast vlan max-group	24-11
ip multicast port max-group	24-13
ip multicast static-neighbor	24-15
ip multicast static-querier	24-17
ip multicast static-group	24-19
ip multicast query-interval	24-21
ip multicast last-member-query-interval	24-23
ip multicast query-response-interval	24-25
ip multicast unsolicited-report-interval	24-27
ip multicast router-timeout	24-29
ip multicast source-timeout	24-31
ip multicast querying	24-33
ip multicast robustness	24-35
ip multicast spoofing	24-37
ip multicast zapping	24-39
ip multicast proxying	24-41
ip multicast helper-address	24-43
ipv6 multicast admin-state	24-44
ipv6 multicast querier-forwarding	24-46
ipv6 multicast version	24-48
ipv6 multicast max-group	24-50
ipv6 multicast vlan max-group	24-52
ipv6 multicast port max-group	24-54
ipv6 multicast static-neighbor	24-56
ipv6 multicast static-querier	24-58
ipv6 multicast static-group	24-60
ipv6 multicast query-interval	24-62
ipv6 multicast last-member-query-interval	24-64
ipv6 multicast query-response-interval	24-66
ipv6 multicast unsolicited-report-interval	24-68
ipv6 multicast router-timeout	24-70
ipv6 multicast source-timeout	24-72
ipv6 multicast querying	24-74
ipv6 multicast robustness	24-76
ipv6 multicast spoofing	24-78
ipv6 multicast zapping	24-80
ipv6 multicast proxying	24-82

show ip multicast	24-84
show ip multicast port	24-89
show ip multicast forward	24-92
show ip multicast neighbor	24-94
show ip multicast querier	24-96
show ip multicast group	24-98
show ip multicast source	24-100
show ip multicast tunnel	24-102
show ipv6 multicast	24-104
show ipv6 multicast port	24-109
show ipv6 multicast forward	24-111
show ipv6 multicast neighbor	24-113
show ipv6 multicast querier	24-115
show ipv6 multicast group	24-117
show ipv6 multicast source	24-119
show ipv6 multicast tunnel	24-121

Chapter 25	DVMRP Commands	25-1
	ip load dvmrp	25-2
	ip dvmrp admin-state	25-3
	ip dvmrp flash-interval	25-4
	ip dvmrp graft-timeout	25-5
	ip dvmrp interface	25-6
	ip dvmrp interface metric	25-7
	ip dvmrp neighbor-interval	25-8
	ip dvmrp neighbor-timeout	25-9
	ip dvmrp prune-lifetime	25-10
	ip dvmrp prune-timeout	25-11
	ip dvmrp report-interval	25-12
	ip dvmrp route-holddown	25-13
	ip dvmrp route-timeout	25-14
	ip dvmrp subord-default	25-15
	ip interface tunnel	25-17
	show ip dvmrp	25-19
	show ip dvmrp interface	25-22
	show ip dvmrp neighbor	25-24
	show ip dvmrp nexthop	25-26
	show ip dvmrp prune	25-28
	show ip dvmrp route	25-30
	show ip dvmrp tunnel	25-32

Chapter 26	PIM Commands	26-1
	ip load pim	26-3
	ip pim sparse admin-state	26-5
	ip pim dense admin-state	26-6
	ip pim ssm group	26-7
	ip pim dense group	26-9
	ip pim cbsr	26-11
	ip pim static-rp	26-13
	ip pim candidate-rp	26-15
	ip pim rp-threshold	26-17
	ip pim keepalive-period	26-18

ip pim max-rps	26-20
ip pim probe-time	26-22
ip pim register checksum	26-23
ip pim register-suppress-timeout	26-24
ip pim spt admin-state	26-25
ip pim state-refresh-interval	26-26
ip pim state-refresh-limit	26-27
ip pim state-refresh-ttl	26-28
ip pim interface	26-29
ip pim neighbor-loss-notification-period	26-32
ip pim invalid-register-notification-period	26-33
ip pim invalid-joinprune-notification-period	26-34
ip pim rp-mapping-notification-period	26-35
ip pim interface-election-notification-period	26-36
show ip pim sparse	26-37
show ip pim dense	26-40
show ip pim ssm group	26-42
show ip pim dense group	26-44
show ip pim neighbor	26-46
show ip pim candidate-rp	26-49
show ip pim group-map	26-51
show ip pim interface	26-53
show ip pim static-rp	26-57
show ip pim cbsr	26-59
show ip pim bsr	26-61
show ip pim notifications	26-63
show ip pim groute	26-66
show ip pim sgroute	26-70
ipv6 pim sparse admin-state	26-75
ipv6 pim dense admin-state	26-76
ipv6 pim ssm group	26-77
ipv6 pim dense group	26-79
ipv6 pim cbsr	26-81
ipv6 pim static-rp	26-83
ipv6 pim candidate-rp	26-85
ipv6 pim rp-switchover	26-87
ipv6 pim spt admin-state	26-88
ipv6 pim interface	26-89
show ipv6 pim sparse	26-92
show ipv6 pim dense	26-94
show ipv6 pim ssm group	26-96
show ipv6 pim dense group	26-98
show ipv6 pim interface	26-100
show ipv6 pim neighbor	26-104
show ipv6 pim static-rp	26-108
show ipv6 pim group-map	26-110
show ipv6 pim candidate-rp	26-112
show ipv6 pim cbsr	26-114
show ipv6 pim bsr	26-116
show ipv6 pim groute	26-118
show ipv6 pim sgroute	26-122

Chapter 27	Multicast Routing Commands	27-1
	ip mroute-boundary	27-3
	ip mroute interface ttl	27-5
	ipv6 mroute interface ttl	27-6
	show ip mroute-boundary	27-7
	show ip mroute	27-9
	show ipv6 mroute	27-11
	show ip mroute interface	27-13
	show ipv6 mroute interface	27-15
	show ip mroute-nexthop	27-17
	show ipv6 mroute-nexthop	27-19
Chapter 28	QoS Commands	28-1
	qos	28-3
	qos trust-ports	28-5
	qos forward log	28-7
	qos log console	28-8
	qos log lines	28-9
	qos log level	28-10
	qos stats interval	28-12
	qos phones	28-13
	qos user-port	28-15
	qos dei	28-18
	debug qos	28-20
	debug qos internal	28-22
	clear qos log	28-24
	qos apply	28-25
	qos revert	28-26
	qos flush	28-27
	qos reset	28-29
	qos stats reset	28-30
	qos port reset	28-31
	qos port	28-32
	qos port trusted	28-34
	qos port maximum egress-bandwidth	28-36
	qos port maximum ingress-bandwidth	28-38
	qos port maximum depth	28-40
	qos port default 802.1p	28-42
	qos port default dscp	28-44
	qos port default classification	28-46
	qos port dei	28-48
	qos qsi qsp	28-50
	qos qsi wred	28-52
	qos qsi stats	28-54
	show qos port	28-56
	show qos slice	28-58
	show qos log	28-60
	show qos config	28-62
	show qos statistics	28-64
	show qos wrp	28-67
	show qos qsp	28-70
	show qos qsi	28-74

show qos qsi stats	28-78
show qos qsi stats rate	28-81
show qos qsi stats bytes	28-83
show qos qsi wred-stats	28-85
clear qos qsi stats	28-87
qos qsp dcb import	28-89
qos qsp dcb tc	28-91
qos qsp dcb tc-numbering	28-93
show qos qsp dcb	28-94
qos qsi dcb dcbx admin-state	28-97
qos qsi qsp dcb	28-99
show qos qsi dcbx	28-101
show qos qsi summary	28-104
qos qsi dcb dcbx ets	28-106
show qos qsi dcb ets	28-108
qos qsi dcb dcbx pfc	28-112
show qos qsi dcbx pfc	28-114
show qos pfc-lossless-usage	28-116
show qos qsi dcb pfc stats	28-117
qos qsi stats admin-state	28-119
show qos qsi stats	28-121
clear qos qsi dcb pfc stats	28-123

Chapter 29

QoS Policy Commands	29-1
policy rule	29-5
policy validity-period	29-9
policy list	29-12
policy list rules	29-14
policy network group	29-16
policy service group	29-18
policy mac group	29-20
policy port group	29-22
policy map group	29-24
policy service	29-26
policy service protocol	29-29
policy service source tcp-port	29-31
policy service destination tcp-port	29-33
policy service source udp-port	29-35
policy service destination udp-port	29-37
policy condition	29-39
policy condition source ip	29-42
policy condition source ipv6	29-44
policy condition destination ip	29-46
policy condition destination ipv6	29-48
policy condition multicast ip	29-50
policy condition source network group	29-52
policy condition destination network group	29-54
policy condition multicast network group	29-56
policy condition source ip-port	29-58
policy condition destination ip-port	29-60
policy condition source tcp-port	29-62
policy condition destination tcp-port	29-64

policy condition source udp-port	29-66
policy condition destination udp-port	29-68
policy condition ethertype	29-70
policy condition established	29-72
policy condition tcpflags	29-74
policy condition service	29-76
policy condition service group	29-77
policy condition icmp type	29-79
policy condition icmp code	29-81
policy condition ip-protocol	29-83
policy condition ipv6	29-85
policy condition nh	29-87
policy condition flow-label	29-89
policy condition tos	29-91
policy condition dscp	29-93
policy condition source mac	29-95
policy condition destination mac	29-97
policy condition source mac group	29-99
policy condition destination mac group	29-101
policy condition source VLAN	29-103
policy condition inner source-vlan	29-104
policy condition destination vlan	29-106
policy condition 802.1p	29-108
policy condition inner 802.1p	29-109
policy condition source port	29-111
policy condition destination port	29-113
policy condition source port group	29-115
policy condition destination port group	29-117
policy condition vrf	29-119
policy condition fragments	29-121
policy action	29-122
policy action disposition	29-124
policy action shared	29-126
policy action priority	29-128
policy action maximum bandwidth	29-130
policy action maximum depth	29-132
policy action cir	29-134
policy action cpu priority	29-137
policy action tos	29-138
policy action 802.1p	29-140
policy action dscp	29-142
policy action map	29-144
policy action permanent gateway-ip	29-146
policy action port-disable	29-148
policy action redirect port	29-150
policy action redirect linkagg	29-152
policy action no-cache	29-154
policy action mirror	29-155
show policy network group	29-157
show policy service	29-159
show policy service group	29-161
show policy mac group	29-163

	show policy port group	29-165
	show policy map group	29-167
	show policy action	29-169
	show policy condition	29-171
	show active policy rule	29-173
	show policy rule	29-175
	show policy validity period	29-177
	show active policy list	29-179
	show policy list	29-181
Chapter 30	Policy Server Commands	30-1
	policy server load	30-2
	policy server flush	30-3
	policy server	30-4
	show policy server	30-6
	show policy server long	30-8
	show policy server statistics	30-10
	show policy server rules	30-12
	show policy server events	30-14
Chapter 31	AAA Commands	31-1
	aaa radius-server	31-3
	aaa tacacs+-server	31-5
	aaa ldap-server	31-7
	aaa authentication	31-10
	aaa authentication default	31-13
	aaa accounting session	31-15
	aaa accounting command	31-17
	aaa device-authentication mac	31-19
	user	31-21
	password	31-24
	user password-size min	31-26
	user password-expiration	31-27
	user password-policy cannot-contain-username	31-29
	user password-policy min-uppercase	31-30
	user password-policy min-lowercase	31-31
	user password-policy min-digit	31-32
	user password-policy min-nonalpha	31-33
	user password-history	31-34
	user password-min-age	31-35
	user lockout-window	31-36
	user lockout-threshold	31-38
	user lockout-duration	31-40
	user lockout unlock	31-42
	show aaa server	31-43
	show aaa authentication	31-46
	show aaa device-authentication	31-48
	show aaa accounting	31-49
	show user	31-50
	show user password-policy	31-53
	show user lockout-setting	31-55
	show aaa priv hexa	31-57

Chapter 32	UNP Commands	32-1
	unp vlan-profile	32-3
	unp port	32-5
	unp default-vlan-profile	32-7
	unp mac-authentication	32-9
	unp mac-authentication pass-alternate	32-11
	unp classification	32-13
	unp port trust-tag	32-15
	unp classification mac-address	32-17
	unp classification mac-range	32-19
	unp classification ip-address	32-21
	unp classification vlan-tag	32-23
	unp dynamic-vlan-configuration	32-25
	unp dynamic-profile-configuration	32-27
	unp auth-server-down-unp	32-29
	unp auth-server-down-timeout	32-30
	show unp	32-31
	show unp global configuration	32-34
	show unp classification	32-37
	show unp port	32-41
	show unp user	32-44
Chapter 33	Edge Virtual Bridging Commands	33-1
	evb type	33-3
	evb evb-ldp manual	33-4
	evb ecp default-ack-timer	33-5
	evb ecp default-max-retry	33-6
	evb vdp default-resource-wait-delay	33-7
	evb vdp default-keep-alive-timeout	33-8
	show evb	33-9
	show evb config	33-11
	show evb sbp-config	33-13
	show evb cdcp-status	33-15
	show evb s-channel	33-17
	show evb ecp-status	33-19
Chapter 34	Port Mapping Commands	34-1
	port-mapping user-port network-port	34-2
	port-mapping	34-4
	port-mapping [unidirectional bidirectional]	34-6
	port-mapping unknown-unicast-flooding	34-8
	show port-mapping status	34-10
	show port-mapping	34-12
Chapter 35	Learned Port Security Commands	35-1
	port-security	35-2
	port-security learning-window	35-4
	port-security convert-to-static	35-7
	port-security maximum	35-9
	port-security learn-trap-threshold	35-11
	port-security port max-filtering	35-13
	port-security mac-range	35-15

	port-security port violation	35-17
	show port-security	35-19
	show port-security brief	35-22
	show port-security learning-window	35-24
Chapter 36	Port Mirroring and Monitoring Commands	36-1
	port-mirroring source destination	36-2
	port-mirroring	36-5
	port-monitoring source	36-7
	port-monitoring	36-10
	show port-mirroring status	36-11
	show port-monitoring status	36-14
	show port-monitoring file	36-16
Chapter 37	sFlow Commands	37-1
	sflow agent	37-3
	sflow receiver	37-4
	sflow sampler	37-6
	sflow poller	37-8
	show sflow agent	37-10
	show sflow receiver	37-12
	show sflow sampler	37-14
	show sflow poller	37-16
Chapter 38	RMON Commands	38-1
	rmon probes	38-2
	show rmon probes	38-4
	show rmon events	38-7
Chapter 39	Switch Logging Commands	39-1
	swlog	39-2
	swlog appid	39-4
	swlog output	39-6
	swlog output flash-file-size	39-8
	swlog clear	39-9
	show log swlog	39-10
	show swlog	39-12
Chapter 40	Health Monitoring Commands	40-1
	health threshold	40-2
	health interval	40-4
	show health configuration	40-5
	show health	40-7
	show health all	40-9
Chapter 41	Ethernet OAM Commands	41-1
	ethoam vlan	41-3
	ethoam domain	41-5
	ethoam domain mhf	41-7
	ethoam domain id-permission	41-8
	ethoam association	41-9
	ethoam association mhf	41-11

ethoam association id-permission	41-13
ethoam association ccm-interval	41-15
ethoam association endpoint-list	41-17
clear ethoam statistics	41-19
ethoam default-domain level	41-20
ethoam default-domain mhf	41-21
ethoam default-domain id-permission	41-22
ethoam default-domain primary-vlan	41-23
ethoam endpoint	41-25
ethoam endpoint admin-state	41-27
ethoam endpoint rfp	41-29
ethoam endpoint ccm	41-31
ethoam endpoint priority	41-33
ethoam endpoint lowest-priority-defect	41-35
ethoam linktrace	41-37
ethoam loopback	41-39
ethoam fault-alarm-time	41-41
ethoam fault-reset-time	41-43
ethoam one-way-delay	41-45
ethoam two-way-delay	41-47
clear ethoam	41-49
show ethoam	41-50
show ethoam domain	41-52
show ethoam domain association	41-54
show ethoam domain association end-point	41-56
show ethoam default-domain configuration	41-59
show ethoam default-domain	41-61
show ethoam remote-endpoint domain	41-63
show ethoam cfmstack	41-65
show ethoam linktrace-reply	41-67
show ethoam linktrace-tran-id	41-70
show ethoam vlan	41-72
show ethoam statistics	41-73
show ethoam config-error	41-75
show ethoam one-way-delay	41-77
show ethoam two-way-delay	41-79

Chapter 42	Service Assurance Agent Commands	42-1
	saa	42-3
	saa type ip-ping	42-5
	saa type mac-ping	42-7
	<i>saa type ethoam-loopback</i>	42-10
	<i>saa type ethoam-two-way-delay</i>	42-13
	saa start	42-15
	saa stop	42-17
	show saa	42-19
	show saa type config	42-21
	show saa statistics	42-25

Chapter 43	VLAN Stacking Commands	43-1
	ethernet-service svlan	43-2
	ethernet-service svlan source-learning	43-4
	ethernet-service service-name	43-6
	ethernet-service nni	43-8
	ethernet-service svlan nni	43-10
	ethernet-service sap	43-12
	ethernet-service sap uni	43-14
	ethernet-service sap cvlan	43-16
	ethernet-service sap-profile	43-18
	ethernet-service sap sap-profile	43-21
	ethernet-service uni-profile	43-23
	ethernet-service uni uni-profile	43-26
	show ethernet-service vlan	43-28
	show ethernet-service	43-30
	show ethernet-service sap	43-33
	show ethernet-service	43-35
	show ethernet-service nni	43-38
	show ethernet-service uni	43-40
	show ethernet-service uni-profile	43-42
	show ethernet-service sap-profile	43-44
Chapter 44	Service Manager Commands	44-1
	service spb	44-3
	service spb description	44-5
	service spb stats	44-7
	service spb admin-state	44-9
	service spb multicast-mode	44-11
	service spb vlan-xlation	44-13
	service spb service-mtu	44-15
	service l2profile	44-17
	service access	44-20
	service access l2profile	44-22
	service access vlan-xlation	44-24
	service spb sap	44-26
	service spb sap description	44-28
	service spb sap trusted	44-30
	service spb sap admin-state	44-32
	service spb sap stats	44-34
	show service l2profile	44-36
	show service access	44-38
	show service	44-40
	show service spb ports	44-42
	show service spb sap	44-44
	show service sdp	44-46
	show service mesh-sdp	44-49
	show service spb debug-info	44-51
	show service spb counters	44-53
	clear service spb counters	44-55

Chapter 45	CMM Commands	45-1
	reload secondary	45-2
	reload all	45-4
	reload from	45-6
	reload slot	45-8
	copy certified	45-9
	issu from	45-10
	issu slot	45-11
	write memory	45-12
	copy running certified	45-13
	modify running-directory	45-15
	copy flash-synchro	45-16
	takeover	45-17
	show running-directory	45-18
	show reload	45-20
	show microcode	45-21
	usb	45-23
	usb auto-copy	45-24
	mount	45-26
	umount	45-27
	show usb statistics	45-28
	show issu status	45-30
Chapter 46	Chassis Management and Monitoring Commands	46-1
	system contact	46-3
	system name	46-4
	system location	46-5
	system date	46-6
	system time	46-7
	system timezone	46-8
	system daylight-savings-time	46-10
	update uboot	46-11
	update fpga	46-12
	reload slot	46-13
	power slot	46-14
	temp-threshold	46-15
	powersupply enable	46-16
	powersupply powersave	46-17
	hash-control	46-18
	license	46-20
	show system	46-21
	show hardware-info	46-23
	show chassis	46-25
	show cmm	46-27
	show slot	46-29
	show module	46-31
	show module long	46-33
	show module status	46-35
	show powersupply	46-37
	show fan	46-39
	show fantray	46-41
	show temperature	46-42

	show hash-control	46-44
	show license-info	46-45
Chapter 47	Chassis MAC Server (CMS) Commands	47-1
	mac-range eeprom	47-2
	show mac-range	47-4
	show mac-range alloc	47-6
Chapter 48	Network Time Protocol Commands	48-1
	ntp server	48-3
	ntp server synchronized	48-5
	ntp server unsynchronized	48-6
	ntp client	48-7
	ntp src-ip preferred	48-8
	ntp broadcast-client	48-10
	ntp broadcast-delay	48-11
	ntp key	48-12
	ntp key load	48-14
	ntp authenticate	48-15
	ntp master	48-16
	ntp interface	48-17
	ntp max-associations	48-18
	ntp broadcast	48-19
	ntp peer	48-21
	ntp vrf-name	48-23
	show ntp status	48-24
	show ntp client	48-27
	show ntp client server-list	48-29
	show ntp server client-list	48-31
	show ntp server status	48-33
	show ntp keys	48-37
	show ntp peers	48-39
	show ntp server disabled-interfaces	48-41
Chapter 49	Session Management Commands	49-1
	session login-attempt	49-3
	session login-timeout	49-4
	session banner	49-5
	session timeout	49-7
	session prompt	49-9
	session xon-xoff	49-10
	show prefix	49-11
	user profile save	49-12
	user profile reset	49-13
	history	49-14
	!	49-15
	command-log	49-17
	kill	49-18
	exit	49-19
	whoami	49-20
	who	49-22
	show session config	49-24

	show session xon-xoff	49-26
	more	49-27
	telnet	49-28
	ssh	49-30
	ssh enforce-pubkey-auth	49-32
	show command-log	49-33
	show command-log status	49-35
	show telnet	49-36
	show ssh	49-37
Chapter 50	File Management Commands	50-1
	cd	50-2
	pwd	50-3
	mkdir	50-4
	rmdir	50-6
	ls	50-8
	rm	50-10
	cp	50-12
	scp	50-14
	mv	50-16
	chmod	50-18
	freespace	50-19
	fsck	50-20
	newfs	50-22
	rcp	50-23
	rrm	50-24
	rls	50-25
	vi	50-27
	tty	50-29
	show tty	50-31
	tftp	50-32
	sftp	50-34
	ftp	50-36
	show ftp	50-38
Chapter 51	Web Management Commands	51-1
	webview server	51-2
	webview access	51-3
	webview force-ssl	51-4
	webview http-port	51-5
	webview https-port	51-6
	show webview	51-7
Chapter 52	Configuration File Manager Commands	52-1
	configuration apply	52-2
	configuration error-file-limit	52-4
	show configuration status	52-6
	configuration cancel	52-8
	configuration syntax-check	52-9
	configuration snapshot	52-11
	show configuration snapshot	52-14
	write terminal	52-17

Chapter 53	SNMP Commands	53-1
	snmp station	53-3
	show snmp station	53-5
	snmp community-map	53-7
	snmp community-map mode	53-9
	show snmp community-map	53-10
	snmp security	53-11
	show snmp security	53-13
	show snmp statistics	53-15
	show snmp mib-family	53-17
	snmp-trap absorption	53-18
	snmp-trap to-webview	53-19
	snmp-trap replay-ip	53-20
	snmp-trap filter-ip	53-22
	snmp authentication-trap	53-24
	show snmp-trap replay-ip	53-25
	show snmp-trap filter-ip	53-27
	show snmp authentication-trap	53-29
	show snmp-trap config	53-30
Chapter 54	DNS Commands	54-1
	ip domain-lookup	54-2
	ip name-server	54-3
	ipv6 name-server	54-5
	ip domain-name	54-7
	show dns	54-8
Appendix A	Software License and Copyright Statements	A-1
	Alcatel-Lucent License Agreement	A-1
	ALCATEL-LUCENT SOFTWARE LICENSE AGREEMENT	A-1
	Third Party Licenses and Notices	A-4
Appendix B	CLI Change Guidelines	B-1
	AOS Release 6 to AOS Release 7	B-1
	List of Changed CLI Commands	B-1
	AAA Commands	B-2
	BFD Commands	B-2
	BGP Commands	B-3
	Configuration File Manager Commands	B-4
	Chassis Management and Monitoring Commands	B-4
	CMM Commands	B-4
	DHCP Relay Commands	B-5
	DVMRP Commands	B-7
	ERP Commands	B-7
	Ethernet Port Commands	B-8
	Health Monitor Commands	B-9
	HTTP Commands	B-9
	IPsec Commands	B-9
	IPv4 Commands	B-9
	IPv6 Commands	B-10

Link Aggregation Commands	B-11
802.1AB Commands	B-13
Multicast Routing Commands	B-14
Network Time Protocol Commands	B-14
OSPF Commands	B-14
OSPFv3 Commands	B-14
PIM Commands	B-14
Port Security Commands	B-15
Policy Server Commands	B-15
Port Manager Commands	B-16
Port Mapping Commands	B-16
Port Mirroring and Monitoring Commands	B-16
QoS Commands	B-17
RIP Commands	B-18
Sflow Commands	B-19
SLB Commands	B-19
SNMP Commands	B-19
Source Learning Commands	B-20
STP Commands	B-20
System Services Command	B-24
VLAN Manager Commands	B-26
VLAN Stacking Commands	B-27
VRRP Commands	B-28
OmniSwitch CLI Short Cuts	B-29
CLI Quick Reference	
Index	Index-1

About This Guide

This *OmniSwitch CLI Reference Guide* is a comprehensive resource to all Command Line Interface (CLI) commands available on the OmniSwitch 10K and OmniSwitch 6900 Series switches.

Supported Platforms

The information in this guide applies only to OmniSwitch 10K and OmniSwitch 6900 switches.

Who Should Read this Manual?

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

When Should I Read this Manual?

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

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

What is in this Manual?

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

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

What is Not in this Manual?

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

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

How is the Information Organized?

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

Text Conventions

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

bold text	Indicates basic command and keyword syntax. Example: show snmp station
<i>italicized text</i>	Indicates user-specific information such as IP addresses, slot numbers, passwords, names, etc. Example: no snmp station <i>ip_address</i> 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 [<i>server_name</i>] Here, you can enter either of the following options: show aaa server show aaa server <i>server_name</i> (where <i>server_name</i> is the user-specified server name, e.g., show aaa server myserver1) Note that this example includes <i>italicized text</i> . The optional parameter in this case is a user-specified server name.
{ } (Curly Braces)	Indicates that the user must choose between one or more parameters. Example: port mirroring {enable disable} Here, you must choose one of the following: port mirroring enable or port mirroring disable
(Vertical Pipes)	Used to separate parameter choices within a command string. For example, the command string show health threshold [rx txrx memory cpu] separates the choices rx , txrx , memory , and cpu . Examples: show health threshold rx show health threshold txrx show health threshold memory show health threshold cpu
“” (Quotation Marks)	Used to enclose text strings that contain spaces. The quotation marks are required input on the command line. Example: vlan 2 “new test vlan”

Documentation Roadmap

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

Stage 1: Using the Switch for the First Time

Pertinent Documentation: *OmniSwitch Getting Started Guide*
Release Notes

A hard-copy *OmniSwitch 10K Getting Started Guide* is included with your switch; this guide provides all the information you need to get your switch up and running the first time. It provides information on unpacking the switch, rack mounting the switch, installing NI modules, unlocking access control, setting the switch's IP address, and setting up a password. It also includes succinct overview information on fundamental aspects of the switch, such as hardware LEDs, the software directory structure, CLI conventions, and web-based management.

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

Stage 2: Gaining Familiarity with Basic Switch Functions

Pertinent Documentation: *OmniSwitch Hardware Users Guide*
OmniSwitch AOS Release 7 Switch Management Guide

Once you have your switch up and running, you will want to begin investigating basic aspects of its hardware and software. Information about switch hardware is provided in the *OmniSwitch 10K Hardware Guide*. This guide provides specifications, illustrations, and descriptions of all hardware components, such as chassis, power supplies, Chassis Management Modules (CMMs), Network Interface (NI) modules, and cooling fans. It also includes steps for common procedures, such as removing and installing switch components.

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

Stage 3: Integrating the Switch Into a Network

Pertinent Documentation: *OmniSwitch AOS Release 7 Network Configuration Guide*
OmniSwitch AOS Release 7 Advanced Routing Configuration Guide

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

The guide includes configuration information for networks using advanced routing technologies (OSPF and BGP) and multicast routing protocols (DVMRP and PIM-SM).

Anytime

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

Related Documentation

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

- *OmniSwitch 10K and OmniSwitch 6900 Getting Started Guides*

Describes the hardware and software procedures for getting an OmniSwitch up and running. Also provides information on fundamental aspects of OmniSwitch software architecture.
- *OmniSwitch 10K and OmniSwitch 6900 Getting Started Guides*

Complete technical specifications and procedures for all OmniSwitch chassis, power supplies, fans, and Network Interface (NI) modules.
- *OmniSwitch CLI Reference Guide*

Complete reference to all CLI commands supported on the OmniSwitch. Includes syntax definitions, default values, examples, usage guidelines and CLI-to-MIB variable mappings.
- *OmniSwitch AOS Release 7 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 7 Network Configuration Guide*

Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols, such as RIP and IPX), security options (authenticated VLANs), Quality of Service (QoS), link aggregation, and server load balancing.
- *OmniSwitch AOS Release 7 Advanced Routing Configuration Guide*

Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package. Chapters cover multicast routing (DVMRP and PIM-SM), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).
- *OmniSwitch Transceivers Guide*

Includes SFP and XFP transceiver specifications and product compatibility information.
- *Technical Tips, Field Notices*

Includes information published by Alcatel-Lucent's Customer Support group.
- *Release Notes*

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

Technical Support

An Alcatel-Lucent service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel-Lucent product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners.

With 24-hour access to Alcatel-Lucent's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel-Lucent's technical support, open a new case or access helpful release notes, technical bulletins, and manuals.

Access additional information on Alcatel-Lucent's Service Programs:

Web: service.esd.alcatel-lucent.com

Phone: 1-800-995-2696

Email: esd.support@alcatel-lucent.com

1 Ethernet Port Commands

The Ethernet port software is responsible for configuring and monitoring Ethernet ports (10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps). This includes:

- Performing hardware diagnostics, loading software, and initializing hardware.
- Notifying other software modules in the system when Ethernet links become active or inactive.
- Configuring basic line parameters for Ethernet ports.
- Gathering basic line statistics for Ethernet ports and passing this information to the user interface and configuration manager.

MIB information for the Ethernet Port commands is as follows:

Filename: AlcatelIND1Port.mib
Module: alcatelIND1PortMIB

Filename: IETF_ETHERLIKE.mib
Module: EtherLike-MIB

A summary of the available commands is listed here.

Interfaces commands

- interfaces**
- interfaces speed**
- interfaces crossover**
- interfaces duplex**
- interfaces alias**
- clear interfaces l2-statistics**
- interfaces max-frame-size**
- interfaces flood-limit**
- interfaces ingress-bandwidth**
- interfaces pause**
- interfaces link-trap**
- interfaces ddm**
- interfaces ddm-trap**
- clear violation**
- show interfaces**
- show interfaces alias**
- show interfaces status**
- show interfaces capability**
- show interfaces accounting**
- show interfaces counters**
- show interfaces counters errors**
- show interfaces flood-rate**
- show interfaces traffic**
- show interfaces ingress-rate-limit**
- show interfaces ddm**
- show transceivers**
- show violation**

interfaces

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

interfaces *{slot/ slot/port[-port2]}* **{admin-state | autoneg | epp}** **{enable|disable}**

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	Last port number in a range of ports you want to configure.
admin-state enable	Enables administrative state.
admin-state disable	Disables administrative state.
autoneg enable	Enables auto negotiation.
autoneg disable	Disables auto negotiation.
epp enable	Enables Enhanced Port Performance.
epp disable	Disables Enhanced Port Performance.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If auto negotiation is disabled, auto MDIX, flow control, auto speed, and auto duplex are not accepted. See the [interfaces crossover](#) command on [page 1-7](#) and the [interfaces duplex](#) command on [page 1-9](#) for more information.
- When EPP is enabled the fiber port receiver performance is enhanced by increasing its sampling rate. This enhancement can help with port link connection reliability or CRC problems that may occur with direct copper cable interfaces.

Examples

```
-> interfaces 3 autoneg disable
-> interfaces 3/1 autoneg disable
-> interfaces 3/1-4 autoneg disable
-> interfaces 2/1-5 admin-state enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces	Configures interface speed.
interfaces crossover	Configures crossover port settings.
interfaces duplex	Enables or disables flow (pause).
show interfaces alias	Displays interface line settings.
show interfaces	Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

esmConfTable

esmPortCfgAutoNegotiation

interfaces speed

Configures interface line speed.

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

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	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 Gigabit.
max 10	Sets the maximum speed to 10 megabits.
max 100	Sets the maximum speed to 100 megabits.
max 1000	Sets the maximum speed to 1000 megabits (1 Gigabit).

Defaults

parameter	default
auto	enable

Platforms Supported

OmniSwitch 10K

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands**show interfaces**

Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

esmConfTable

esmPortCfgSpeed

interfaces crossover

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

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

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	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	auto

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If auto negotiation is disabled, then automatic crossover is also disabled. See the [interfaces](#) command for more information.
- You cannot configure crossover settings on fiber ports. These ports use the MDI standard.

Examples

```
-> interfaces 3 crossover mdi
-> interfaces 3/1 crossover mdix
-> interfaces 3/1-4 crossover auto
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces](#)

Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

```
esmConfTable
  esmPortCfgCrossover
```

interfaces duplex

Configures duplex mode. In full duplex mode, the interface transmits and receives data simultaneously. In half duplex mode, the interface can transmit *or* receive data at a given time. Auto duplex setting causes the switch to advertise all available duplex modes (half/full/both) for the port during autonegotiation.

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

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	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 auto-negotiation.

Defaults

parameter	default
full half auto	full

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- Half duplex mode is not supported on Gigabit modules if a port is detected as Gigabit (1000 Mbps).
- Gigabit and 10 Gigabit fiber ports only support full duplex.

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[interfaces](#)

Configures interface line speed. Set to **auto** to set speed and duplex mode to auto-sensing.

[show interfaces](#)

Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

esmConfTable

esmPortAutoDuplexMode

interfaces alias

Configures a description (alias) for a single port.

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

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>description</i>	A description for the port, which can be up to 40 characters long. Description tags with spaces must be enclosed within quotes (e.g., "IP Phone").

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 (e.g., "").

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces alias](#) Displays port status (up or down) and any aliases for a port.

MIB Objects

ifXTable
ifAlias

clear interfaces l2-statistics

Resets all statistics counters.

```
clear interfaces {slot / slot/port[-port2]} l2-statistics [cli]
```

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	Last port number in a range of ports you want to configure.
cli	Clears the CLI statistics only.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> clear interfaces 3/1 l2-statistics  
-> clear interfaces 3/2 l2-statistics cli
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces counters](#) Displays general interface information, including when statistics were last cleared.

MIB Objects

alCetherStatsTable
alCetherClearStats

interfaces max-frame-size

Configures the maximum frame size for Gigabit Ethernet interfaces.

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

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	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
<i>bytes</i> (Gigabit Ethernet Packets)	9216
<i>bytes</i> (Ethernet Packets)	1553

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces](#) Displays auto negotiation, speed, duplex, and crossover settings.

MIB Objects

esmConfTable
esmPortCfgMaxFrameSize

interfaces flood-limit

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

interfaces {*slot/ slot/port[-port2]*} **flood-limit** {**bcast|mcast|uucast|all**} **rate** { **pps** *pps_num* | **mbps** *mbps_num* | **cap%** *cap_num* | **enable** | **disable**}

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	Last port number in a range of ports you want to configure.
bcast	Specifies broadcast flood limit.
mcast	Specifies multicast flood limit.
uucast	Specifies unicast flood limit.
all	Specifies flood limit for all types of traffic.
<i>pps_num</i>	Packets per second.
<i>mbps_num</i>	Megabits per second.
<i>cap_num</i>	Percentage of port's capacity.
enable	Enables flood rate limits.
disable	Disables flood rate limits.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> interfaces 3 flood-limit all rate cap% 50
-> interfaces 2/1 flood-limit bcast rate mbps 100
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces flood-rate](#) Displays interface flood rate settings.

MIB Objects

```
esmConfigTable
  esmPortCfgFlow
dot3PauseTable
  dot3PauseAdminMode
```

interfaces ingress-bandwidth

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

```
interfaces {slot/ slot/port[-port2]} ingress-bandwidth {mbps| enable | disable}
```

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	Last port number in a range of ports you want to configure.
mbps	Speciifies the ingress bandwidth in mpbs.
enable	Enables ingress bandwidth limiting.
disable	Disables ingress bnadwidth limiting.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> interfaces 3 ingress-bandwidth enable
-> interfaces 3 ingress-bandwidth mbps 30
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces ingress-rate-limit](#) Displays the ingress-rate-limit set for each interface por.

MIB Objects

interfaces pause

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

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

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	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.
disable	Disables flow control on the interface.

Platforms Supported

OmniSwitch 10K, 6900

Defaults

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

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. Note that the operational settings override the configured settings as long as autonegotiation and flow control are both enabled for the interface:
- If autonegotiation is disabled, the configured flow control settings are applied to the local interface.

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces status](#)

Displays interface line settings.

MIB Objects

esmConfigTable

 esmPortCfgFlow

dot3PauseTable

 dot3PauseAdminMode

interfaces link-trap

Enables trap link messages. If enabled, a trap is generated whenever the port changes state.

```
interfaces [slot | slot/port [-port2]] link-trap {enable|disable}
```

Syntax Definitions

<i>slot</i>	Slot number you want to configure.
<i>port</i>	Port number of the interface you want to configure.
<i>port2</i>	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.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces status](#) Displays interface line settings.

MIB Objects

```
esmConfigTable
  esmPortSlot
  esmPortIF
```

interfaces ddm

Configures the DDM administrative status.

```
interfaces ddm {enable | disable}
```

Syntax Definitions

enable	Enables DDM functionality.
disable	Disables DDM functionality.

Defaults

parameter	default
ddm	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- DDM capability will vary based on the transceiver manufacturer.
- DDM status must be enabled in order to enable traps; traps are enabled separately.

Examples

```
-> interfaces ddm enable  
-> interfaces ddm disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces ddm](#) Displays the interface DDM status.

MIB Objects

```
ddmConfiguration  
  ddmConfig
```

interfaces ddm-trap

Configures the DDM administrative status or trap capability.

```
interfaces ddm-trap {enable | disable}
```

Syntax Definitions

enable	Enables DDM trap functionality.
disable	Disables DDM trap functionality.

Defaults

parameter	default
ddm-trap	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

DDM status must be enabled in order to enable traps; traps are enabled separately.

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces ddm](#) Displays the interface DDM status.

MIB Objects

```
ddmConfiguration
  ddmTrapConfig
  ddmNotificationType
```

clear violation

Clears all the MAC address violation logs for a particular port and session. After the violations are cleared, the specific port resumes normal operation. This includes applying an existing application configuration.

```
clear violation {port slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id[-agg_id2]</i>	Enter a link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When a violation is set on a physical port that is part of a link aggregate, the violation is set for the whole link aggregate. All ports on that link aggregate are brought down. When this command is applied to a link aggregate ID, all member ports of the link aggregate are activated.
- When this command is applied, all MAC addresses known to the port are cleared from the MAC address table for the switch.

Examples

```
-> clear violation port 1/10
-> clear violation port 2/1-5
-> clear violation linkagg 5
-> clear violation linkagg 10-20
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show violation](#) Displays the address violations that occur on ports with LPS restrictions.

MIB Objects

```
portViolationTable
  portViolationClearPort
```

show interfaces

Displays general interface information (e.g., hardware, MAC address, input errors, and output errors).

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The Link-Quality parameter and Enhanced Port Performance capabilities are only supported on the OS6900.

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                 : GBIC_SX,
EPP                     : Disabled,, Link-Quality:Good
MAC address             : 00:d0:95:b2:39:85,
BandWidth (Megabits)    : 1000,                Duplex          : Full,
Autonegotiation         : 1 [ 1000-F 100-F 100-H 10-F 10-H ],
Long Accept             : Enable,                Runt Accept     : Disable,
Long Frame Size(Bytes) : 9216,                Runt Size(Bytes) : 64,
Rx
Bytes Received          :          7967624, Unicast Frames :          0,
Broadcast Frames:      :          124186, M-cast Frames  :          290,
UnderSize Frames:      :          0, OverSize Frames:    :          0,
Lost Frames             :          0, Error Frames      :          0,
CRC Error Frames:      :          0, Alignments Err   :          0,
Tx
Bytes Xmitted           :          255804426, Unicast Frames :          24992,
Broadcast Frames:      :          3178399, M-cast Frames  :          465789,
UnderSize Frames:      :          0, OverSize Frames:    :          0,
Lost Frames             :          0, Collided Frames:   :          0,
```

output definitions

Slot/Port	Interface slot and port.
Operational Status	Interface status (up/down).
Last Time Link Changed	The last time the configuration for this interface was changed.
Number of Status Change	The total number of times that the configuration of this interface has changed.
Type	Interface type (Ethernet/Fast Ethernet/Gigabit Ethernet).
SFP/XFP	The type of transceiver detected.
EPP	Enhanced Port Performance setting.
Link-Quality	The link quality of the connection: GOOD - The port will connect with no problems and transfer data with no errors. FAIR - The port may have intermittent problems connecting and maintaining its connection to a remote port and/or intermittent CRC's could occur. POOR - The port will have problems connecting and maintaining a connection with remote port. If the ports connect, it's likely CRC errors will occur. N/A - The port link quality is either very poor or the port type does not support the Link Quality capability.
MAC address	Interface MAC address.
Bandwidth	Bandwidth (in megabits).
Duplex	Duplex mode (Half/Full/Auto).
Autonegotiation	The auto negotiation settings for this interface.
Long Accept	Long Frames status (enable/disable).
Runt Accept	Runt Frames status (enable/disable).
Long Frame Size	Long Frame Size (in Bytes).
Runt Size	Runt Frame Size (in Bytes).
Bytes Received	Number of Bytes received.
Rx Unicast Frames	Number of unicast frames received.
Rx Broadcast Frames	Number of broadcast frames received.
Rx M-cast Frames	Number of multicast frames received.
Rx Undersize Frames	Number of undersized frames received.
Rx Oversize Frames	Number of oversized frames received.
Rx Lost Frames	Number of Lost Frames received.
Rx Error Frames	Number of error frames received.
Rx CRC Error Frames	Number of CRC error frames received. Only applies to frames that are less than or equal to Max/Long Frame Size. Frames larger than Long Frame Size are counted as OverSizeFrames.
Rx Alignments Err	Number of Alignments Error frames received.
Bytes Xmitted	Number of Bytes transmitted.

output definitions (continued)

Tx Unicast Frames	Number of unicast frames transmitted.
Tx Broadcast Frames	Number of broadcast frames transmitted.
Tx M-cast Frames	Number of multicast frames r transmitted.
Tx Undersize Frames	Number of undersized frames transmitted.
Tx Oversize Frames	Number of oversized frames transmitted.
Tx Lost Frames	Number of Lost Frames transmitted.
Tx Collided Frames	Number of collision frames received or transmitted.
Tx Error Frames	Number of error frames transmitted.

Release History

Release 7.1.1; command introduced.

Related Commands

show interfaces accounting	Displays interface accounting information (e.g., packets received/transmitted).
show interfaces counters	Displays interface counter information (e.g., unicast packets received/transmitted).
show interfaces alias	Displays the interface line settings (e.g., speed and mode).
show interfaces traffic	Displays interface traffic statistics (input/output bytes and packets).

MIB Objects

ifTable

- ifOperStatus
- ifType
- ifPhysAddress
- ifSpeed
- ifInDiscards
- IfOutDiscards

esmConfTable

- esmPortSlot
- esmPortIF
- esmPortCfgLongEnable
- esmPortCfgRuntEnable
- esmPortCfgMaxFrameSize
- esmPortCfgRuntSize

ifXTable

- ifHCInOctets
- ifHCInUcastPkts
- ifHCInBroadcastPkts
- ifHCInMulticastPkts
- IfHCOutOctets
- IfHCOutUcastPkts
- IfHCOutBroadcastPkts
- IfHCOutMulticastPkts

alcetherStatsTable

- alcetherStatsRxUndersizePkts
- alcetherStatsCRCAlignErrors
- alcetherStatsTxUndersizePkts
- alcetherStatsTxOversizePkts
- alcetherStatsTxCollisions

dot3StatsTable

- dot3StatsFrameTooLong
- dot3StatsFCSErrors
- dot3StatsLateCollisions

show interfaces alias

Displays interface line settings (e.g., speed and mode).

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If no slot/port numbers are entered, line settings for all slots/ports on the switch are displayed.

Examples

```
-> show interfaces 1/2 alias
```

```
Slot/   Admin   Link   Alias
Port    Status  Status
-----+-----+-----+-----
 1/1    disable  down   ""
```

output definitions

Slot/Port	Interface slot/port number.
Admin Status	The administrative status of the port.
Link Status	The link status of the port. Autonegotiation status (Enable/Disable).
Alias	The configured alias for the port..

Release History

Release 7.1.1; command introduced.

Related Commands[interfaces alias](#)

Configures the port alias.

MIB Objects

```
ifXTable
  ifAlias
```

show interfaces status

Displays interface line settings (e.g., speed and mode).

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If no slot/port numbers are entered, line settings for all slots/ports on the switch are displayed.

Examples

```
-> show interfaces 1/2 status
```

Slot/ Port	Admin Status	Auto Nego	DETECTED-VALUES			CONFIGURED-VALUES			Link Trap
			Speed (Mbps)	Duplex	Pause	Speed (Mbps)	Duplex	Pause	
1/1	dis	en	-	-	-	Auto	Auto	-	dis

output definitions

Slot/Port	Interface slot/port number.
Admin Status	The administrative status of the port.
AutoNego	Autonegotiation status (Enable/Disable).
Detected Speed	Detected line speed in Mbps.
Detected Duplex	Detected line duplex (Half duplex/Full duplex/Auto).
Detected Pause	Detected pause control configuration.
Configured Speed	Configured line speed (10/100/Auto/1000/10000 Mbps).
Configured Duplex	Configured line duplex (Half duplex/Full duplex/Auto).
Configured Pause	Detected pause control configuration.
Link Trap	Link Trap status.

Release History

Release 7.1.1; command introduced.

Related Commands

[interfaces](#)

Enables/disables Trap LinkUpDown.

[interfaces](#)

Configures interface line speed, sets speed, and duplex mode to auto-sensing.

[interfaces duplex](#)

Configures interface duplex mode.

MIB Objects

ifTable

 ifLinkUpDownTrapEnable

esmConfTable

 esmPortSlot

 esmPortIF

 esmPortAutoSpeed

 esmPortAutoDuplexMode

 esmPortCfgSpeed

 esmPortCfgDuplexMode

show interfaces capability

Displays default auto negotiation, speed, duplex, flow, and cross-over settings for a single port, a range of ports, or all ports on a Network Interface (NI) module.

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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      Pause      Crossover      Speed      Duplex
-----+-----+-----+-----+-----+-----
 5/1  CAP      EN/DIS      EN/DIS      MDI/X/Auto  10/100/1G  Full/Half
 5/1  DEF              EN          EN           Auto         Auto       Auto
```

output definitions

Slot	The slot number.
Port	The port number
AutoNeg	In the row labeled CAP , the field displays the valid auto negotiation configurations for the port. In the row label DEF , the field displays the default auto negotiation settings for the port. The possible values are EN (enabled) or DIS (disabled).
Pause	In the row labeled CAP , the field displays the valid pause configurations for the port. In the row label DEF , the field displays the default pause settings for the port.

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 , 1G , 10/100/1G , 10G , or Auto .
Duplex	In the row labeled CAP , the field displays the valid duplex configurations for the port. In the row label DEF , the field displays the default duplex settings for the port. The possible values are Full , Full/Half , or Auto .

Release History

Release 7.1.1; command introduced.

Related Commands

interfaces	Enables and disables auto negotiation.
interfaces crossover	Configures crossover port settings.
interfaces	Configures interface speed.
interfaces duplex	Configures duplex settings.
show interfaces alias	Displays interface line settings.

MIB Objects

```
esmConfTable
  esmPortCfgAutoNegotiation
  esmPortCfgFlow
  esmPortCfgCrossover
  esmPortCfgSpeed
  esmPortAutoDuplexMode
```

show interfaces accounting

Displays interface accounting information (e.g., packets received/transmitted and deferred frames received).

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If no slot/port numbers are entered, accounting information for all slots/ports on the switch is displayed.

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.

output definitions (continued)

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 7.1.1; command introduced.

Related Commands

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

MIB Objects

esmConfTable

esmPortSlot

esmPortIF

dot3StatsTable

dot3StatsFrameTooLong

dot3StatsDeferredTransmissions

alcetherStatsTable

alcetherStatRxsUndersizePkts

alcetherStatTxUndersizePkts

alcetherStatsTxOversizePkts

alcetherStatsPkts64Octets

alcetherStatsPkts65to127Octets

alcetherStatsPkts128to255Octets

alcetherStatsPkts256to511Octets

alcetherStatsPkts512to1023Octets

alcetherStatsPkts1024to1518Octets

gigaEtherStatsPkts1519to4095Octets

gigaEtherStatsPkts4096to9215Octets

 alcetherStatsRxJabber

show interfaces counters

Displays interface counters information (e.g., unicast, broadcast, and multi-cast packets received/transmitted).

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If no slot/port numbers are entered, counter information for all slots/ports on the switch is displayed.

Examples

```
-> show interfaces 3/1 counters
```

```
InOctets      = 54367578586897979,  OutOctets      = 5.78E19,
InUcastPkts   = 55654265276,    OutUcastPkts   = 5.78E20,
InMcastPkts   = 58767867868768777,  OutMcastPkts   = 5465758756856,
InBcastPkts   = 576567567567567576,  OutBcastPkts   = 786876,
InPauseFrames = 567798768768767,    OutPauseFrames = 786876,
```

output definitions

InOctets	Number of octets received.
OutOctets	Number of octets transmitted.
InUcastPkts	Number of unicast packets received.
OutUcastPkts	Number of unicast packets transmitted.
InMcastPkts	Number of multicast packets received.
OutMcastPkts	Number of unicast packets transmitted.
InBcastPkts	Number of broadcast packets received.
OutBcastPkts	Number of unicast packets transmitted.
InPauseFrames	Number of MAC control frames received.
OutPauseFrames	Number of MAC control frames transmitted.

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

esmConfTable

 esmPortSlot

 esmPortIF

ifXTable

 IfHCInOctets

 IfHCOctets

 IfHCInUcastPkts

 IfHCOctetsUcastPkts

 IfHCInMulticastPkts

 IfHCOctetsMulticastPkts

 IfHCInBroadcastPkts

 IfHCOctetsBroadcastPkts

dot3PauseTable

 dot3InPauseFrame

 dot3OutPauseFrame

show interfaces counters errors

Displays interface error frame information (e.g., CRC errors, transit errors, and receive errors).

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If no slot/port numbers are entered, counter error information for all slots/ports on the switch is displayed.

Examples

```
-> show interfaces 2/1 counters errors
```

```
02/01,
  Alignments Errors = 6.45E13,  FCS Errors = 7.65E12
  IfInErrors        = 6435346,  IfOutErrors= 5543,
  Undersize pkts    = 867568,  Oversize pkts= 5.98E8
```

output definitions

Slot/Port	Interface slot and port number.
Alignments Errors	Number of Alignments errors.
FCS Errors	Number of Frame Check Sequence errors.
IfInErrors	Number of received error frames.
IfOutErrors	Number of transmitted error frames.
Undersize pkts	Number of undersized packets.
Oversize pkts	Number of oversized packets (more than 1518 octets).

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces counters](#)

Displays interface counters information (e.g., unicast, broadcast, and multi-cast packets received/transmitted).

MIB Objects

```
esmConfTable
  esmPortSlot
  esmPortIF
ifTable
  ifInErrors
  ifOutErrors
alcetherStatsTable
  alcetherStatsRxUndersizePkts
dot3StatsTable
  dot3StatsAlignmentErrors
  dot3StatsFCSErrors
  dot3StatsFrameTooLong
```

show interfaces flood-rate

Displays interface peak flood rate settings.

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show interfaces flood-rate
Slot/  Bcast   Bcast   Bcast   Ucast   Ucast   Ucast   Mcast   Mcast   Mcast
Port  Value    Type    Status  Value    Type    Status  Value    Type    Status
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
1/1      496  mbps  enable      496  mbps  enable      496  mbps  disable
1/2      496  mbps  enable      496  mbps  enable      496  mbps  disable
1/3      496  mbps  enable      496  mbps  enable      496  mbps  disable
1/4      496  mbps  enable      496  mbps  enable      496  mbps  disable
1/5      496  mbps  enable      496  mbps  enable      496  mbps  disable
```

output definitions

Slot/Port	Interface slot and port numbers.
Value	The value set based on the type of flood limiting.
Type	The type of flood limiting: mbps, pps, or %
Status	Status of the type of flood-limiting: enabled or disabled.

Release History

Release 7.1.1; command introduced.

Related Commands

[interfaces flood-limit](#)

Configures the peak flood rate for an interface.

MIB Objects

```
esmConfTable  
  esmPortSlot  
  esmPortIF  
  esmPortMaxFloodRate  
  esmPortFloodMcastEnable
```

show interfaces traffic

Displays interface traffic statistics.

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

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port2</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If no slot/port numbers are entered, traffic settings for all slots/ports on the switch are displayed.

Examples

```
-> show interfaces traffic
Slot/Port   Input packets   Input bytes   Output packets   Output bytes
-----+-----+-----+-----+-----
1/2         322             20624        5125             347216
3/2         322             20620        5133             347764
```

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 7.1.1; command introduced.

Related Commands

[interfaces ddm](#)

Displays general interface information (e.g., hardware, MAC address, and input/output errors).

[show interfaces counters](#)

Displays interface counter information (e.g., unicast packets received/transmitted).

MIB Objects

esmConfTable

 esmPortSlot

 esmPortIF

ifXTable

 ifHCInOctets

 ifHCInUcastPkts

 ifHCInMulticastPkts

 ifHCInBroadcastPkts

 ifHCOctets

 ifHCOUcastPkts

 ifHCOMulticastPkts

 ifHCOBroadcastPkts

show interfaces ingress-rate-limit

Displays the ingress-rate-limit set for each interface port.

show interfaces [*slot*/ *slot/port*[-*port1*]] **ingress-rate-limit**

Syntax Definitions

<i>slot</i>	Slot number you want to display.
<i>port</i>	Port number of the interface you want to display.
<i>port1</i>	Last port number in a range of ports you want to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If the slot number is not specified, then the switch back pressure feature must be enabled or disabled on an entire chassis.

Examples

```
-> show interfaces 1/1-4 ingress-rate-limit
Slot/ Rate Limit Burst Size Status
Port   (Mbps)      (MB)
-----+-----+-----+-----
1/1      496           19  disable
1/2      496           19  disable
1/3      496           19  disable
1/4      496           19  disable
```

output definitions

Slot/Port	Interface slot and port numbers.
Rate Limit (Mbps)	Rate limit in Megabits.
Burst Size (MB)	Burst size in Megabytes.
Status	Status of rate limiting.

Release History

Release 7.1.1; command introduced.

Related Commands[interfaces duplex](#)

Configures the ingress-rate-limit.

MIB Objects

```
esmConfTable
  esmPortSlot
  esmPortIF
```

show interfaces ddm

Displays the information for the specified transceivers.

show interfaces [*slot* | *slot/port*[-*port1*]] **ddm** [**W-LOW** **W-HIGH** **STATUS** **A-LOW** **A-HIGH** **ACTUAL**]

Syntax Definitions

<i>slot</i>	Display all the transceivers on the specified slot.
<i>num</i>	Display information for the specified transceiver.
<i>port2</i>	Last port number in a range of ports to display.
W-LOW	Display the transceivers Warning Low value.
W-HIGH	Display the transceivers Warning High value.
STATUS	Display the administrative status of DDM.
A-LOW	Display the transceivers Alarm Low value.
A-HIGH	Display the transceivers Alarm High value.
ACTUAL	The real-time values indicated by the transceiver. Values displayed in parentheses indicate the Warning or Alarm value that has been reached.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If the threshold values of the transceiver are '0' then NS (Not Supported) will be displayed in the DDM output display.

Examples

```
-> show interfaces transceiver W-Low
```

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

```
-> show interfaces transceiver A-High
```

```
Slot/Port Temp C Voltage(V) Current(mA) Output(dBm) Input(dBm)
-----+-----+-----+-----+-----+-----+

```

```

1/1      50      5.75      75      3.22      3.22
1/2      50      5.95      65      3.22      3.22
1/3      NA      NA      NA      NA      NA

```

```
-> show interfaces 1/1 transceiver
```

```

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

```

```
-> show interfaces transceiver ddm
```

```

DDM Status      : enable
DDM Trap Status : disable

```

output definitions

Slot/Port	Interface slot and port numbers.
Temp C	The transceiver temperature, in degrees centigrade.
Voltage (V)	The transceiver supply voltage, in volts.
Current (mA)	The transceiver transmit bias current, in milliamps.
Output (dBm)	The transceiver output power, in decibels.
Input (dBm)	The transceiver received optical power, in decibels.
DDM Status	The administrative status of DDM.
DDM Trap Status	The administrative status of DDM traps.
Actual	The real-time values indicated by the transceiver. Values displayed in parentheses indicate the Warning or Alarm value that has been reached.
Alarm High (AH)	Indicates the value at which the transceiver's functionality may be affected.
Warning High (WH)	Indicates the transceiver is approaching the High Alarm value.
Warning Low (WL)	Indicates the transceiver is approaching the Low Alarm value.
Alarm Low (AL)	Indicates the value at which the transceiver's functionality may be affected.
N/A	Indicates the transceiver does support DDM.
N/S	Indicates the transceiver does not support the DDM attribute.

Release History

Release 7.1.1; command introduced.

Related Commands

[show interfaces ddm](#)

Configures the DDM administrative status or trap capability.

MIB Objects

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

show transceivers

Displays transceiver manufacturer and status information.

show transceivers [*slot slot*]

Syntax Definitions

slot Display all the transceivers on the specified slot.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show transceivers
Slot 2 Transceiver 1
  Manufacturer Name:      FIBERXON INC.      ,
  Part Number:           FTM-8012C-SLG      ,
  Hardware Revision:     10                  ,
  Serial Number:         101680092800319    ,
  Manufacture Date:      090707,
  Laser Wave Length:     850nm,
  Admin Status:          POWER ON,
  Operational Status:    UP
```

output definitions

Manufacturer Name	The name of the transceiver's manufacturer.
Part Number	The part number of the transceiver.
Hardware Revision	The hardware revision of the transceiver.
Serial Number	The serial number of the transceiver.
Manufacturer Date	The manufacture date of the transceiver.
Laser Wave Length	The laser wavelength of the transceiver.
Admin Status	The administrative status of the transceiver.
Operational Status	The operational status of the transceiver.

Release History

Release 7.1.1; command introduced.

Related Commands[show interfaces ddm](#)

Displays the DDM administrative status or trap capability.

MIB ObjectsN/A

show violation

Displays the address violations that occur on ports with LPS restrictions. This command displays a port violation for sticky port security when the maximum number of MAC address of the connected workstation that the switch learns.

show violation {port *slot/port*[-*port2*] | linkagg *agg_id*[-*agg_id2*]}

Syntax Definitions

slot/port[-*port2*] The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

agg_id[-*agg_id2*] Enter a link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

NA

Examples

-> show violation

Port	Source	Action	Reason	Timer
1/1	src lrn	simulated down	lps shutdown	0
1/1	src lrn	simulated down	lps restrict	0
2	qos	admin down	policy	0

The **admin down** action in the **show violation** output for link aggregate 2 indicates that a port violation has occurred on one of the ports related to the link aggregate group with ID 2.

output definitions

Port	The slot and port numbers or link aggregate IDs on which address violations occurred
Source	Specifies the source application that detected the violation.
Action	Specifies the action that is taken when the violation is detected on the port. There are two types of actions: admin down - deactivates the physical port. simulated down - the port is put in blocking state.

output definitions

Reason	Specifies the reason for the violation.
Timer	Specifies the duration of the violation timer.

Release History

Release 7.1.1; command introduced.

Related Commands

clear violation Clears all the MAC address violation logs for a particular port and session. After the violations are cleared, the specific port resumes normal operation.

MIB Objects

```
portViolationTable
  portViolationSource
  portViolationEntry
  portViolationTrap
  portViolationSource
  portViolationReason
  portViolationAction
  portViolationTimer
  portViolationTimerAction
```

2 UDLD Commands

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

The two basic mechanisms that UDLD follows are:

- Advertises port 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
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 “Configuring UDLD,” *OmniSwitch 10K 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 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command 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
  alaUdldGlobalConfigUdldStatus
```

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

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

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command 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

alaUdldPortConfigUdldStatus

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

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

Defaults

parameter	default
normal aggressive	normal

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The UDLD protocol must be enabled before using this command.
- The UDLD protocol is not supported on aggregate ports.
- In case of faulty cable connection, the port which is configured in normal mode of operation is considered 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 7.1.1; command 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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>port2</i>	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).
<i>seconds</i>	The probe-message transmission interval, in seconds.

Defaults

parameter	default
<i>seconds</i>	15

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command 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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>port2</i>	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).
<i>seconds</i>	The echo based detection period, in seconds.

Defaults

parameter	default
<i>seconds</i>	8

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command 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 udd statistics port

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

clear udd statistics [*port slot/port*]

Syntax Definitions

slot/port

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

uddl

Globally enables or disables UDLD protocol on the switch.

show udd statistics port

Displays the UDLD statistics for a specific port.

MIB Objects

alaUddGlobalClearStats

show uddl configuration

Displays the global status of UDLD configuration.

show uddl configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show uddl configuration
```

```
Global UDLD Status           : disabled,
Global UDLD Mode             : normal,
Global UDLD Probe Timer (Sec) : 15,
Global UDLD Echo-Wait Timer (Sec) : 8
Global UDLD Status : Disabled
```

output definitions

Global UDLD Status	Indicates the UDLD status on the switch. Options include enabled or disabled .
Global UDLD Mode	Indicates the UDLD mode on the switch. Options include normal or aggressive .
Global UDLD Probe Timer (Sec)	A probe-message is expected after this time period.
Global UDLD Echo-Wait Timer (Sec)	The detection of neighbor is expected with in this time period.
Global UDLD Status	Indicates the UDLD status on the switch. Options include enabled or disabled .

Release History

Release 7.1.1; command introduced.

Related Commands

udld

Globally enables or disables UDLD protocol on the switch.

show udd configuration port

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

MIB Objects

alaUddGlobalStatus

alaUddGlobalConfigUddStatus

show udld configuration port

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

show udld configuration port [*slot/port*]

Syntax Definitions

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

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

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	aggressive	55	8
1/21	disabled	aggressive	55	8
1/22	disabled	aggressive	55	8
1/41	disabled	aggressive	77	8
1/42	enabled	aggressive	77	8
1/43	enabled	aggressive	77	8
1/44	enabled	aggressive	77	8
1/45	enabled	aggressive	77	8

```
-> show udld configuration port 1/44
```

```
Global UDLD Status           : enabled,
Port UDLD Status             : enabled,
Port UDLD State              : bidirectional,
UDLD Op-Mode                 : aggressive,
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	A probe-message is expected after this time period.
Echo-Wait Timer	The detection of neighbor is expected with in this time period.

Release History

Release 7.1.1; command 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
  alaUdldGlobalConfigUdldStatus
alaUdldPortConfigTable
  alaUdldPortConfigUdldOperationalStatus
  alaUdldPortConfigUdldMode
  alaUdldPortConfigUdldStatus
  alaUdldPortConfigUdldProbeIntervalTimer
  alaUdldPortConfigUdldDetectionPeriodTimer
alaUdldPortNeighborStatsTable
  alaUdldNeighborName

```

show uddl statistics port

Displays the UDLD statistics for a specific port.

show uddl statistics port *slot/port*

Syntax Definitions

slot/port

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show uddl 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 7.1.1; command 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 uddl neighbor port

Displays the UDLD neighbor ports.

show uddl neighbor port *slot/port*

Syntax Definitions

slot/port

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

-> show uddl 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 7.1.1; command introduced.

Related Commands

udld echo-wait-timer

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

show udld statistics port

Displays the UDLD statistics for a specific port.

MIB Objects

alaUdldPortNeighborStatsTable

alaUdldNeighborName

show udld status port

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

show udld status port [*slot/port*]

Syntax Definitions

slot/port

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

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

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

MIB Objects

alaUdldGlobalStatus
alaUdldPortConfigTable
alaUdldPortConfigUdldOperationalStatus

3 Source Learning Commands

The Source Learning capability of OmniSwitch 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-learning**
- mac-learning flush**
- mac-learning flush domain**
- mac-learning static mac-address**
- mac-learning multicast mac-address**
- mac-learning aging-time**
- mac-learning mode**
- mac-ping**
- show mac-learning**
- show mac-learning remote**
- show mac-learning aging-time**
- show mac-learning learning-state**
- show mac-learning mode**

mac-learning

Configures the status of source MAC address learning on a single port, a range of ports, or on a link aggregate of ports.

mac-learning {port *slot/port* / linkagg *linkagg*} {enable | disable}

Syntax Definitions

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>linkagg</i>	Specifies the link aggregate ID number.
enable	Enables source learning.
disable	Disables source learning.

Defaults

By default, source learning is enabled on all ports.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Configuring source learning is not supported on Learned Port Security (LPS) and Universal Network Profile (UNP) ports, as well as individual ports that are members of a link aggregate.
- 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, dynamic learning of MAC addresses is stopped.
- 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 on which source learning is disabled.
- Disabling source learning on a port or link aggregate is useful on a ring configuration, where switch A does not have to learn MAC addresses from switch B, or for a Transparent LAN Service, where service provider does not require the MAC addresses of the customer network.

Examples

```
-> mac-learning port 1/2 enable
-> mac-learning linkagg 10 disable
```

Release History

Release 7.1.1; command added.

Related Commands

show mac-learning learning-state

Displays the source learning status of a port or link aggregate on the switch.

Related MIB Objects

slMacLearningControlTable
slMacLearningControlStatus

mac-learning flush

Clears the specified MAC addresses from the Source Learning MAC Address Table on the local switch.

mac-learning flush {dynamic | static | multicast} [**mac-address** *mac_address*]

Syntax Definitions

dynamic	Clears dynamically learned MAC addresses.
static	Removes static MAC addresses.
multicast	Removes static multicast MAC addresses.
<i>mac_address</i>	Enter the MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c).

Defaults

Platforms Supported

parameter	default
mac-address	all MAC addresses

OmniSwitch 10K, 6900

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table.
- Static unicast and static multicast addresses are removed. This command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush vlan 20 port 1/2 dynamic
-> mac-learning flush vlan 20 linkagg 10 static
```

Release History

Release 7.3.1; command added.

Related Commands

[show mac-learning](#) Displays Source Learning MAC Address Table information for the local switch.

Related MIB Objects

slMacLearningControlTable
slMacLearningControlStatus

mac-learning flush domain

Clears the specified MAC addresses from the Source Learning MAC Address Table for the specified learning domain on the local switch.

mac-learning flush domain {**all** | **vlan** {**vlan** *vlan_id* [**port** *slot/port* | **linkagg** *agg_id*]} | **spb** {**serviceid** *service_id* | **sap** *slot/port:encap* | **mesh-sdp** *mesh_id* | **isid** *instance_id*} | **evb** {**serviceid** *service_id*}} {**dynamic** | **static** | **static-multicast**} [**mac-address** *mac_address*]

Syntax Definitions

all	Selects all learning domains.
vlan	Selects the VLAN domain.
<i>vlan_id</i>	VLAN ID number.
<i>slot/port</i>	The slot and port number (3/1) that is assigned to the static MAC address.
<i>linkagg_id</i>	Enter a link aggregate ID number. See Chapter 8, “Link Aggregation Commands.”
spb	Selects the Shortest Path Bridging (SPB) service domain.
<i>service_id</i>	An existing SPB service ID.
<i>slot/port:encap</i>	The SPB access port and encapsulation (0 , all , <i>qtag</i> , or <i>outer_qtag.inner_qtag</i>) for a SPB service access point (SAP).
<i>mesh_id</i>	A SPB service distribution point (SDP) ID.
<i>isid instance_id</i>	A SPB backbone service instance identifier (I-SID).
evb	Selects the Shortest Path Bridging (SPB) service domain.
<i>service_id</i>	An existing Edge Virtual Bridging (EVB) service ID.
dynamic	Clears dynamically learned MAC addresses from the specified domain.
static	Removes static MAC addresses from the specified domain.
static-multicast	Removes static multicast MAC addresses from the specified domain. This parameter is not available for use with the all , spb , or evb parameters.
<i>mac_address</i>	Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

Defaults

parameter	default
mac-address	all MAC addresses

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the specific domain.
- Static unicast and static multicast addresses are removed.
- The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

Examples

```
-> mac-learning flush domain vlan vlan 20 port 1/2 dynamic
-> mac-learning flush domain vlan linkagg 10 static
-> mac-learning flush domain spb sap 1/12:0 dynamic
-> mac-learning flush domain all
```

Release History

Release 7.3.1; command added.

Related Commands

[mac-learning flush](#)

Clears the MAC Address Table for the local switch.

[show mac-learning](#)

Displays Source Learning MAC Address Table information for the local switch.

Related MIB Objects

```
slMacLearningControlTable
slMacLearningControlStatus
```

mac-learning static mac-address

Configures a static destination unicast MAC address. The configured MAC address is assigned to a fixed switch port or link aggregate ID and VLAN. If the destination of the data packets received on the VLAN ports is the configured MAC address, then they are forwarded to the specific MAC address port.

mac-learning {vlan *vlan_id* {port *slot/port* | linkagg *linkagg_id*} static mac-address *mac_address* [bridging | filtering]

mac-learning flush [vlan *vlan_id* [port *slot/port* | linkagg *linkagg_id*]] static [mac-address *mac_address*]

Syntax Definitions

<i>vlan_id</i>	VLAN ID number.
<i>slot/port</i>	The slot and port number (3/1) that is assigned to the static MAC address.
<i>linkagg_id</i>	Enter a link aggregate ID number. See Chapter 8, “Link Aggregation Commands.”
static	Specifies a permanent static MAC address that is retained even after the switch reboots.
dynamic	Specifies a dynamic MAC address that is removed when the switch reboots.
<i>mac_address</i>	Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
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 filtered or dropped.

Defaults

parameter	default
bridging filtering	bridging

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **mac-learning flush** command to remove a static MAC address from the Source Learning MAC Address Table. Note that if no parameters are specified with this command, then all static addresses are removed.
- Enter a port number or link aggregate ID that is already associated with the specified VLAN ID. Only traffic from other ports associated with the same VLAN is directed to the static MAC address 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.
- The destination MAC addresses are maintained in the Source Learning MAC address table.
- If a packet received on a port associated with the same VLAN contains a source address that matches a static MAC address, then the packet is discarded.

Examples

```
-> mac-learning vlan 10 port 1/10 static mac-address 00:00:39:59:f1:0c bridging
-> mac-learning vlan 20 linkagg 5 static mac-address 00:00:9a:55:e0:01 filtering
-> mac-learning flush vlan 500 static
-> mac-learning flush vlan 10 port 1/10 static mac-address 00:00:39:59:f1:0c
-> mac-learning flush vlan 20 linkagg 5 static
-> mac-learning flush static
```

Release History

Release 7.1.1; command introduced.

Release 7.3.1: **mac-learning flush** command replaced the **no mac-learning** command.

Related Commands

[vlan members untagged](#)

Assigns ports and link aggregates to a VLAN.

[mac-learning multicast mac-address](#)

Configures a static multicast MAC address and assigns the address to one or more egress ports or link aggregates.

[show mac-learning](#)

Displays Source Learning MAC Address Table information.

MIB Objects

```
alaSlMacAddressGlobalTable
  slOriginId
  slServiceId
  slMacAddressGbl
  slMacAddressGblManagement
  slMacAddressGblDisposition
```

mac-learning multicast mac-address

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-learning {vlan *vlan_id* { port *slot/port* | linkagg *linkagg_id* }} **multicast mac-address** *multicast_address* [**group** *group_id*]

mac-learning flush [vlan *vlan_id* [port *slot/port* | linkagg *linkagg_id*]] **multicast** [**mac-address** *multicast_address*]

Syntax Definitions

<i>vlan_id</i>	VLAN ID number.
<i>slot/port</i>	The egress slot and port number (3/1) that is assigned to the static multicast MAC address.
<i>linkagg_id</i>	Enter a link aggregate ID number. See Chapter 8, “Link Aggregation Commands.”
<i>multicast_address</i>	Enter the destination multicast MAC Address to add to the MAC Address Table (for example, 01:00:39:59:f1:0c).
<i>group_id</i>	<i>This keyword cannot be user defined.</i>

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **mac-learning flush** command to remove a static multicast MAC address from the Source Learning MAC Address Table. Note that if no parameters are specified with this 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-learning vlan multicast mac-address** 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 fixed switch port or link aggregate ID and VLAN.
- 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.
- Enter a port number or link aggregate ID that is already associated with the specified VLAN ID. Only traffic from other ports associated with the same VLAN is directed to the static MAC address 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 “**group group_id**” as the additional syntax for the **mac-learning static-multicast** command. The “**group group_id**” 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.
- 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-learning vlan 1500 port 1/10 multicast mac-address 03:00:00:3a:44:12
-> mac-learning vlan 355 port 4/2-10 multicast mac-address 02:00:39:59:f1:0c
-> mac-learning vlan 455 linkagg 10 multicast mac-address 04:00:00:3a:44:13
-> mac-learning flush vlan 500 multicast
-> mac-learning flush vlan 1500 port 1/10 multicast mac-address 03:00:00:3a:44:12
-> mac-learning flush vlan 455 linkagg 10 multicast mac-address 04:00:00:3a:44:13
-> mac-learning flush multicast
```

Release History

Release 7.1.1; command introduced.

Release 7.3.1; **mac-learning flush** command replaced the **no mac-learning** command.

Related Commands

vlan members untagged	Assigns ports and link aggregates to a VLAN.
mac-learning static mac-address	Configures a static MAC address and assigns the address to a port or link aggregate.
show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
alaSlMacAddressGlobalTable
  slOriginId
  slServiceId
  slMacAddressGbl
  slMacAddressGblManagement
  slMacAddressGblDisposition
```

mac-learning 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-learning aging-time {*seconds* | **default**}

no mac-learning aging-time

Syntax Definitions

seconds Aging time value (in seconds). Do not use commas in value.

default The aging time is set to the default value of 300 seconds.

Defaults

By default, the aging time is set to 300 seconds.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **default** parameter 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.
- Note that an inactive MAC address can take up to twice as long as the aging time value specified to be removed from the MAC address table. For example, if an aging time of 60 seconds is specified, the MAC address ages out any time between 60 and 120 seconds of inactivity.
- 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-learning aging-time 1200  
-> mac-learning aging-time default
```

Release History

Release 7.1.1; command introduced.

Related Commands

show mac-learning

Displays Source Learning MAC Address Table information.

show mac-learning aging-time

Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

slMacAddressAgingTable

slMacAgingValue

mac-learning mode

Specifies the source learning mode for the chassis.

mac-learning mode [centralized | distributed]

Syntax Definitions

centralized Enables centralized MAC source learning mode.

distributed Enables distributed MAC source learning mode.

Defaults

By default, centralized MAC source learning mode is enabled for the chassis.

Platforms Supported

OmniSwitch 10K

Usage Guidelines

After the distributed MAC mode is either enabled or disabled using this command, immediately save the switch configuration using the **write memory** command and then reboot the switch.

Examples

```
-> mac-learning mode centralized
-> mac-learning mode distributed
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show mac-learning mode](#) Displays the current status of the MAC source learning mode.

MIB Objects

slDistributedMacMode

show mac-learning

Displays Source Learning MAC Address Table information for the local switch.

show mac-learning [**summary**] [**multicast** | **static** | **dynamic**] [**vlan** *vlan_id* [-*vlan_id2*]] [**slot** *slot* | **port** *slot/port*] [**linkagg** *agg_id*] [**mac-address** *mac_address*]

Syntax Definitions

summary	Displays summary of all the parameters.
multicast	Displays all the static multicast MAC addresses information contained in the MAC address table.
static	Displays static MAC addresses with a permanent status.
dynamic	Displays dynamically learned MAC addresses.
<i>vlan_id</i> [- <i>vlan_id2</i>]	VLAN ID number. Use a hyphen to specify a range of VLAN ID numbers (1-20).
<i>slot</i>	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).
<i>slot/port</i>	The slot and port number (3/1).
<i>agg_id</i>	The link aggregate ID number.
<i>mac_address</i>	MAC Address (for example, 00:00:39:59:f1:0c).

Defaults

By default, information is displayed for all MAC addresses contained in the table.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the **show mac-learning** 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.
- If there is a duplicate static MAC address occurrence, a “&” will appear to the right of the address in the **show mac-learning** command display.

Examples

```
-> show mac-learning summary
Mac Address Table Count:
  Permanent Address Count           = 0,
  Dynamic Learned Address Count     = 16,
  Static Multicast Address Count    = 0,
```

Total MAC Address In Use = 16

-> show mac-learning

Legend: Mac Address: * = address not valid
 Mac Address: & = duplicate static address,

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-learning vlan 10-15

Legend: Mac Address: * = address not valid
 Mac Address: & = duplicate static address,

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	remote
12	00:d0:95:ad:e3:cc	learned	---	bridging	remote
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 the slot/port.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status: dynamic or static .
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 .
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). In an MCLAG configuration, this field displays remote if the address was learned on a fixed port of the MCLAG peer switch.

Release History

Release 7.1.1; command introduced.

Related Commands

- show mac-learning remote** Displays MAC addresses learned on a Multi-Chassis Link Aggregation (MCLAG) peer switch.
- show mac-learning aging-time** Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable  
  slOriginId  
  slServiceId  
  slMacAddressGbl  
  slMacAddressGblManagement  
  slMacAddressGblDisposition  
  slMacAddressGblProtocol
```

show mac-learning remote

Displays Source Learning MAC Address Table information for devices learned on a fixed port connected to the remote (peer) switch in a Multi-Chassis Link Aggregation (MCLAG) network configuration.

```
show mac-learning [summary | multicast | static | dynamic] [vlan vlan_id [-vlan_id2]] {remote
[mac_address]}
```

Syntax Definitions

summary	Displays a summary of remote permanent (static), dynamic, and static multicast MAC address information.
multicast	Display all the static multicast MAC addresses information contained in the MAC address table.
static	Display static MAC addresses with a permanent status.
dynamic	Display dynamically learned MAC addresses.
<i>vlan_id</i> [- <i>vlan_id2</i>]	VLAN ID number. Use a hyphen to specify a range of VLAN ID numbers (1-20).
<i>mac_address</i>	Enter a MAC Address (for example, 00:00:39:59:f1:0c).

Defaults

By default, information is displayed for all remote MAC addresses contained in the table.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the **show mac-learning** 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.
- If there is a duplicate static MAC address occurrence, a “&” will appear to the right of the address in the show mac-learning command display.

Examples

```
-> show mac-learning remote
Legend: Mac Address: * = address not valid
       Mac Address: & = duplicate static address,
```

Vlan	Mac Address	Type	Protocol	Operation	Interface
1	00:00:00:11:00:01	dynamic	---	bridging	remote
1	00:00:00:11:00:03	static	---	bridging	remote

Total number of Valid MAC addresses above = 3

```
-> show mac-learning summary remote
Mac Address Table Count:
Permanent Address Count      = 0,
Dynamic Learned Address Count = 2,
Static Multicast Address Count = 0,
Total MAC Address In Use     = 0
```

```
-> show mac-learning vlan 10-15 remote
Legend: Mac Address: * = address not valid
        Mac Address: & = duplicate static address,
```

Vlan	Mac Address	Type	Protocol	Operation	Interface
12	00:d0:95:a8:2a:b6	learned	---	bridging	Remote
12	00:d0:95:ad:e3:cc	learned	---	bridging	Remote

Total number of Valid MAC addresses above = 2

output definitions

VLAN	Vlan ID number associated with the MAC address and the slot/port.
Mac Address	MAC address that is currently learned or statically assigned.
Type	MAC address management status: dynamic or static .
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 .
Interface	The slot and port number 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). In an MCLAG configuration, this field displays remote if the address was learned on a fixed port of the MCLAG peer switch.

Release History

Release 7.1.1; command introduced.

Related Commands

show mac-learning	Displays source learning MAC address table information.
show mac-learning aging-time	Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

```
alaSlMacAddressGlobalTable
  slOriginId
  slServiceId
  slMacAddressGbl
  slMacAddressGblManagement
  slMacAddressGblDisposition
  slMacAddressGblProtocol
```

show mac-learning aging-time

Displays the current aging time value for the Source Learning MAC Address Table.

```
show mac-learning aging-time
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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-learning aging-time  
Mac Address Aging Time (seconds) = 300
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show mac-learning](#) Displays Source Learning MAC Address Table information.

MIB Objects

```
s1MacAddressAgingTable  
s1MacAgingValue
```

show mac-learning learning-state

Displays the source learning status of a VLAN, port or link aggregate.

```
show mac-learning learning-state [vlan vlan[-vlan2] / port slot/port | linkagg linkagg]
```

Syntax Definitions

<i>vlan</i>	The VLAN ID number.
<i>-vlan2</i>	The last VLAN ID in a range of VLAN IDs.
<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>linkagg</i>	Specifies the link aggregate identifier.

Defaults

By default, the source learning status for all switch ports and link aggregates is displayed.

Platforms Supported

OmniSwitch 10K

Usage Guidelines

- Use the **port** or **linkagg** keywords along with the port ID and link aggregate ID to display the source learning status for a specific port or link aggregate ID.
- Use the **vlan** keyword along with the VLAN ID or a range of VLAN IDs to display the source learning status for the specified VLAN or range of VLANs.
- Output display for a range of port IDs is supported with this command. However, output display for a range of link aggregate IDs is not supported.
- 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 mac-learning learning-state

port  mac-learning
-----+-----
1/1   disabled
1/2   enabled
1/3   disabled

-> show mac-learning learning-state port 1/2

port  mac-learning
-----+-----
1/2   enabled
```

```
-> show mac-learning learning-state linkagg 10
```

```
port    mac-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).
mac-learning	The source learning status of the port or link aggregate (enabled or disabled). Configured through the mac-learning command.

```
-> show mac-learning learning-state vlan 1-5
```

```
      Vlan      Learning State
-----+-----
          1      Enabled
          5      Enabled
```

output definitions

Vlan	The VLAN ID numbers of the VLANs that are active.
Learning State	The MAC learning state of the VLANs.

Release History

Release 7.1.1; command introduced

Related Commands

mac-learning Configures the status of source MAC address learning on a single port, a range of ports or on a link aggregate of ports.

Related MIB Objects

```
s1MacAddressTable
s1MacLearningControlTable
  s1MacLearningControlEntry
  s1MacLearningControlStatus
```

show mac-learning mode

Displays the current source learning mode (centralized or distributed) for the switch.

show mac-learning mode

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show mac-learning mode
MAC Learning Mode Configuration = CENTRALIZED
New Configured MAC Learning Mode After Reboot = DISTRIBUTED

-> show mac-learning mode
MAC Learning Mode Configuration = DISTRIBUTED
```

Release History

Release 7.1.1; command introduced.

Related Commands

[mac-learning mode](#) Enables or disables the distributed MAC source learning mode.

MIB Objects

```
s1MacAddressTable
  s1DistributedMacMode
```

mac-ping

Configure a MAC address ping for testing layer 2 connectivity.

```
mac-ping dst-mac mac vlan vlan-id [priority vlan-priority] [drop-eligible {true | false}] [count count]
[interval delay] [size size] [isid-check isid]
```

Syntax Definitions

<i>mac</i>	The destination MAC address to ping.
<i>vlan-id</i>	The VLAN on which the packets will be sent out. Valid range is 1-4094.
<i>vlan-priority</i>	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.
<i>count</i>	The number of packets to send in one ping iteration. Valid range is 1-5.
<i>delay</i>	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.
<i>size</i>	The size of the ICMP payload to be used for the ping iteration. Valid range is 32-1500 bytes.
<i>isid</i>	A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network.

Defaults

parameter	default
<i>vlan-priority</i>	0
<i>drop-eligible</i>	false
<i>count</i>	5
<i>delay</i>	1000 ms
<i>size</i>	36 bytes

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The timeout for each ping request packet is 1 sec. This value is not configurable.
- Destination MAC cannot be a broadcast, multicast, or NULL address.

Examples

```
-> mac-ping dst-mac 00:11:11:11:11:11 vlan 10  
-> mac-ping dst-mac 00:11:11:11:11:11 vlan 10 count 5 size 100  
-> mac-ping dst-mac 00:11:11:11:11:11 vlan 1001 isid-check 1002
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show mac-learning](#) Displays Source Learning MAC Address Table information.

MIB Objects

N/A

4 VLAN Management Commands

VLAN management software handles VLAN configuration and the reporting of VLAN configuration changes to other switch tasks. A VLAN defines a broadcast domain that contains physical ports and can span across multiple switches. All switches contain a default VLAN 1. Physical switch ports are initially assigned to VLAN 1 until they are statically or dynamically assigned to other VLANs.

This chapter includes descriptions of VLAN management commands used to create, modify or remove VLANs. These commands allow you to enable or disable Spanning Tree Protocol (STP), add or remove virtual router interfaces, statically assign physical switch ports to a default VLAN, and display VLAN configuration information.

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 members untagged](#)
[vlan members tagged](#)
[vlan mtu-ip](#)
[show vlan](#)
[show vlan members](#)

vlan

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

vlan *vlan_id* [**admin-state** {**enable** | **disable**}] [**name** *description*]

no vlan *vlan_id*

Syntax Definitions

<i>vlan_id</i>	A numeric value that uniquely identifies an individual VLAN. This value becomes the VLAN ID for the new VLAN.
enable	Enable VLAN administrative status.
disable	Disable VLAN administrative status.
description	An alphanumeric string. Optional name description for the VLAN ID.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

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. If the VLAN deleted is a default VLAN on the port, the port returns to default VLAN 1.
- If the VLAN deleted is not a default VLAN, then the ports are directly detached from the VLAN.
- A VLAN is not operationally active until at least one of the member ports of the VLAN is active and can forward traffic.
- 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 of VLAN ID entries (for example, vlan 10-15).
- When a VLAN is administratively disabled, static port assignments are retained but traffic is not forwarded from these ports.
- The description can be any alphanumeric string. Enclose the description in double quotes if it contains more than one word with space in between.

Examples

```
-> vlan 200 name "Corporate VLAN"  
-> vlan 720 admin-state disable  
-> no vlan 1020
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan members untagged	Statically assigns ports to a VLAN.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
vlanTable  
  vlanNumber  
  vlanDescription  
  vlanAdmStatus  
  vlanOperStatus  
  vlanStatus
```

vlan members untagged

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 vlan_id [-vlan_id2] members {port slot/port[-port1] | linkagg linkagg_id[-linkagg_id2]} untagged
```

```
no vlan vlan_id [-vlan_id2] members {port slot/port[-port1] | linkagg_id linkagg_id[-linkagg_id2]}
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number of the VLAN to assign as the default VLAN configured for the port.
<i>slot/port</i> [- <i>port1</i>]	The slot number for the module and the physical port number (for example, 3/1 specifies port 1 on slot 3) or a range of physical port numbers on that module (for example, 3/1-16).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number or range of IDs to be assigned to the specified VLAN.

Defaults

VLAN 1 is the default VLAN for all ports.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a port or link aggregate from its configured default VLAN and restore VLAN 1 as the default VLAN.
- The VLAN ID and link aggregate ID specified with this command must already exist in the switch configuration.
- This command configures the port or link aggregate to send and receive untagged packets for the specified VLAN ID, which becomes the default VLAN of the port.
- Every switch port or link aggregate has only one configured default VLAN. The 802.1Q tagged ports, however, can have additional VLAN assignments, which are often referred to as *secondary* VLANs.

Examples

```
-> vlan 20 members port 4/1-24 tagged
-> vlan 20 members linkagg 2-4 untagged
-> no vlan 1-4 members port 4/1-24
-> no vlan 20 members linkagg 2-4
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan	Creates a VLAN.
vlan members tagged	Configures a port to accept 802.1q-tagged packets for a specific VLAN.
show vlan	Displays list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

vpaTable
 vpaVlanNumber
 vpaIfIndex
 vpaType
 vpaState
 vpaStatus

vlan members tagged

Configures a port or link aggregate ID to send and receive 802.1q-tagged packets with the specified VLAN ID.

vlan *vlan_id*[-*vlan_id2*] **members** {**port** *slot/port*[-*port2*] | **linkagg** *linkagg_id*[-*linkagg_id2*]} **tagged**

no vlan *vlan_id*[-*vlan_id2*] **members** {**port** *slot/port*[-*port2*] | **linkagg** *linkagg_id*[-*linkagg_id2*]}

Syntax Definitions

<i>vlan_id</i>	The VLAN ID number for a preconfigured VLAN that will handle the 802.1Q-tagged traffic for this port. The valid range is 1–4094.
<i>slot</i>	The slot number for the 802.1Q tagging.
<i>port</i>	The port number for the 802.1Q tagging.
<i>-port2</i>	The last port number in a range of ports.
<i>linkagg_id</i>	The link aggregation ID, which allows you to configure 802.1Q tagging on an aggregate of ports. The valid range is 1 to 31.
<i>-linkagg_id2</i>	The last link aggregate ID in a range.

Defaults

By default, all ports are untagged (they only carry untagged traffic for the default VLAN to which the port belongs).

Platforms Supported

OmniSwitch 10K

Usage Guidelines

- Use the **no** form of this command to delete 802.1Q tagging on a port or an aggregate of ports.
- The VLAN ID and link aggregate ID specified with this command must already exist in the switch configuration.
- A port or link aggregate cannot be tagged with its own default VLAN ID.

Examples

```
-> vlan 2 members port 3/1 tagged
-> vlan 100 members port 4/1-10
-> vlan 100 members linkagg 10
-> vlan 100 members linkagg 1-4
-> no vlan 2 members port 3/1
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan	Creates a VLAN.
vlan members untagged	Configures the default VLAN for the specified port or link aggregate.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
qPortVlanTable
  qPortVlanSlot
  qPortVlanPort
  qPortVlanStatus
  qPortVlanTagValue
  qPortVlanDescription
  qAggregateVlanTagValue
  qAggregateVlanAggregateId
  qAggregateVlanStatus
  qAggregateVlanDescription
```

vlan mtu-ip

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

vlan *vlan_id* **mtu-ip** *size*

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number of the VLAN to assign as the default VLAN configured for the port.
<i>size</i>	Packet size value specified in bytes.

Defaults

By default, the MTU size is set to 1500 bytes (the standard Ethernet MTU size).

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The MTU size applies to traffic sent on all switch ports that are associated with the specified VLAN regardless of the port speed (for example, 10/100 Ethernet, gigabit Ethernet). Therefore, assign only ports that are capable of handling the MTU size restriction to the VLAN. If the VLAN MTU size is greater than 1500, do not assign 10/100 Ethernet ports to the VLAN.
- By default, packets that exceed the MTU size are dropped. To enable MTU discovery and fragmentation, use the **icmp type** command to enable the “frag needed but DF bit set” control (for example, **icmp type 3 code 4 enable**).
- The maximum MTU size value for a Multi-chassis MCM-IPC VLAN is 9198.

Examples

```
-> vlan 200 mtu-ip 1000
-> vlan 1503 mtu-ip 9198
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan	Creates a VLAN.
vlan members tagged	Configures a port to accept 802.1q-tagged packets for a specific VLAN.
show vlan	Displays list of existing VLANs.

MIB objects

vlanTable
vlanMtu

show vlan

Displays a list of VLANs configured on the switch.

```
show vlan [vlan_id]
```

Syntax Definitions

vlan_id VLAN ID number.

Defaults

By default, a list of all VLANs is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Specify a VLAN ID with this command to display information about a specific VLAN.
- Note that specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, show vlan 10-15). Note that only one VLAN entry - a single VLAN ID or a range of VLAN IDs is allowed with this command. Multiple entries are not accepted.

Examples

```
-> show vlan
```

```

vlan  type  admin  oper  ip   mtu   name
-----+-----+-----+-----+-----+-----+-----
   1   std    Ena    Dis   Dis  1500  Finance IP
  10  unpd   Ena    Dis   Dis  1500  UNP-DYN-VLAN
  11   std    Ena    Dis   Dis  1500  VLAN 11

```

output definitions

vlan	The numerical VLAN ID. Use the vlan command to create or remove VLANs.
type	The type of VLAN (mtp , ipc , std , vip , unpd).
admin	VLAN administrative status: Ena specifies that VLAN functions are enabled; Dis specifies that VLAN functions are disabled. Use the vlan command to change the VLAN administrative status.
oper	VLAN operational status: Ena (enabled) or Dis (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)

ip	IP router interface status: Ena (IP interface exists for the VLAN) or Dis (no IP router interface exists for the VLAN). Use the ip interface command to define an IP router interface for a VLAN.
mtu	Maximum Transmission Unit: Size of largest data packet that the VLAN port can transmit. Configured through the vlan mtu-ip command.
name	The user-defined text description for the VLAN. By default, the VLAN ID is displayed if the VLAN description is not specified. Configured through the vlan command.

```
-> show vlan 10
```

```
Name                : UNP-DYN-VLAN,
Type                : UNP Dynamic Vlan,
Administrative State : enabled,
Operational State   : disabled,
IP Router Port      : disabled,
IP MTU              : 1500
```

output definitions

Name	The user-defined text description for the VLAN. By default, the VLAN ID is displayed if the VLAN description is not specified.
Type	The type of VLAN (Static Vlan, MTP Vlan, MCM IPC, VIP Vlan, UNP Dynamic VLAN)
Administrative State	VLAN administrative status: enabled VLAN functions are enabled; disabled specifies that VLAN functions are disabled. Use the vlan command to change the VLAN administrative status.
Operational State	VLAN operational status: Ena (enabled) or Dis (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.
IP Router Port	IP router port status: Ena (IP interface exists for the VLAN) or Dis (no IP router interface exists for the VLAN). Use the ip interface command to define an IP router interface for a VLAN.
IP MTU	Maximum Transmission Unit: Size of largest data packet that the VLAN port can transmit.

Release History

Release 7.1.1; command introduced.

Related Commands

[show vlan members](#) Displays VLAN port assignments.

MIB Objects

vlanMgrVlan

vlanTable

 vlanNumber

 vlanDescription

 vlanAdmStatus

 vlanOperStatus

 vlanStatus

show vlan members

Displays VLAN port associations (VPAs) for all VLANs, a specific VLAN, or for a specific port.

```
show vlan [vlan_id [-vlan_id2]] members [port [slot/port[-port2]/ linkagg linkagg_id [-linkagg_id2]]
```

Syntax Definitions

<i>vlan_id</i>	VLAN ID number.
<i>-vlan_id2</i>	The last VLAN ID in a range of VLAN IDs.
<i>slot/port</i>	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).
<i>linkagg_id</i>	Enter the link aggregate ID number to assign to the specified VLAN.
<i>linkagg_id2</i>	The last link aggregate ID in a range of IDs to be assigned to a 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 10K, 6900

Usage Guidelines

- If the *vlan_id* is specified without a *slot/port* or *linkagg_id*, then all port assignments for that VLAN are displayed.
- If the *slot/port* or *linkagg_id* is specified without a *vlan_id*, then all VLAN assignments for that port are displayed.
- If both the *vlan_id* and *slot/port* or *linkagg_id* are specified, then information only for that VLAN and *slot/port* or link aggregate ID is displayed.
- Note that specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, show vlan 10-15 port). Note that only one VLAN entry - a single VLAN ID or a range of VLAN IDs is allowed with this command. Multiple entries are not accepted.

Examples

```
-> show vlan members
vlan  port      type      status
+-----+-----+-----+-----+
  1    1/1      default   inactive
  2    1/2      default   blocking
      11/4     qtagged   forwarding
  3    1/2      qtagged   blocking
      11/4     default   forwarding
      2/5      dynamic   forwarding
```

```
-> show vlan 10 members
port  type      status
+-----+-----+-----+
 1/1  default   forwarding
 1/2  qtagged   forwarding
```

```
-> show vlan members port 3/2
vlan  type      status
+-----+-----+-----+
  1    default   forwarding
  2    qtagged   forwarding
  5    dynamic   blocking
  3    qtagged   blocking
```

```
-> show vlan 1-11 members port 1/3
type      : default,
status     : inactive,
vlan admin : enabled,
vlan oper  : disabled,
```

output definitions

vlan	Numerical VLAN ID. Identifies the VLAN assignment of the port.
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), mirror (port is mirroring the VLAN assignment of another port), dynamic (configured dynamic VLAN assignment for the port).
status	The VPA status: inactive (port is not active), forwarding (traffic is forwarding on this VPA), blocking (traffic is not forwarding on this VPA)
vlan admin	VLAN administrative status: enabled enables VLAN functions to operate; disabled disables VLAN functions without deleting the VLAN. Use the vlan command to change the VLAN administrative status.
vlan oper	VLAN operational status: enabled or 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.

Release History

Release 7.1.1; command introduced.

Related Commands

[show vlan](#) Displays list of VLANs configured on the switch.
[show ip interface](#) Displays IP router information.

MIB Objects

vlanMgrVpa
vpaTable
 vpaVlanNumber
 vpaIfIndex
 vpaType
 vpaState
 vpaStatus
vlanMgrVlan
vlanTable
 vlanAdmStatus
 vlanOperStatus

5 High Availability VLAN Commands

High availability (HA) VLANs send traffic intended for a single destination MAC address to multiple switch ports. The OmniSwitch HA VLAN feature provides an elegant and flexible way to connect server cluster nodes directly to the ingress network. This involves multicasting the service requests on the configured ports. The multicast criteria is configurable based on destination MAC and destination IP address. Egress ports can be statically configured on a server cluster or they can be registered by IGMP reports. The HA VLAN server cluster feature multicasts the incoming packets based on the server cluster configuration on the ports associated with the server cluster.

An HAVLAN is configured by specifying the match criteria, a VLAN and a port list. Match criteria is used to identify the incoming traffic that has to be processed by the HA VLAN server-clusters. The specified VLAN is an ingress and egress VLAN in the case of a L2 server-cluster. In the case of a L3 server-cluster, the VLAN is not configured explicitly, but the IP address specified in the match criteria determines the VLAN. The port list specifies the egress switch ports within the VLAN. The cluster is connected to these switch ports.

There are typically two modes of implementation of server clusters in HA VLAN.

Layer 2 - The server cluster is attached to a L2 switch on which the frames destined to the cluster MAC address are to be flooded on all interfaces.

Layer 3 - The server cluster is attached to a L3 switch on which the frames destined to the server cluster IP address are to be routed to the server cluster IP and then flooded on all interfaces.

For more information, see the application examples in Chapter 28, “Configuring High Availability VLANs” in the *OmniSwitch AOS Release 7 Network Configuration Guide*.

MIB information is as follows:

Filename: AlcatelIND1VlanManager.mib
Module: ALCATEL-IND1-VLAN-MGR-MIB

Filename: AlcatelIND1MacAddress.mib
Module: ALCATEL-IND1-MAC-ADDRESS-MIB

A summary of the available commands is listed here:

[server-cluster](#)
[server-cluster vlan](#)
[server-cluster mac-address](#)
[server-cluster ip](#)
[server-cluster igmp mode](#)
[server-cluster ip-multicast](#)
[server-cluster port](#)
[show server-cluster](#)

server-cluster

Configures a cluster with an ID, name, mode and the administrative state.

server-cluster *cluster-id* [**name** *cluster-name*] [**mode** {**L2** | **L3**}] [**admin-state** {**enable**|**disable**}]

no server-cluster *cluster-id*

Syntax Definitions

<i>cluster-id</i>	A numerical identifier of the cluster. The valid range is 1–32.
<i>cluster-name</i>	Specifies a name (up to 32 characters) to represent the cluster.
L2	Specifies L2 for the cluster mode.
L3	Specifies L3 for the cluster mode.
enable	Enables the administrative state of the cluster.
disable	Disables the administrative state of the cluster.

Defaults

parameter	default
mode	L2
admin-state	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use **no** form of this command to remove the cluster ID from the switch configuration.
- Once the cluster mode is set, the mode cannot be changed.
- Use the **admin-state disable** parameter option to disable an existing cluster before attempting to modify any of the cluster parameters.

Examples

```
-> server-cluster 1
-> server-cluster 1 mode l2
-> server-cluster 1 name l2_cluster mode l2
-> server-cluster 2 name l3_cluster mode l3
-> no server-cluster 1
```

Release History

Release 7.2.1; command was introduced.

Related Commands

vlan	Creates and deletes VLANs.
server-cluster mac-address	Configures a MAC address, VLAN of the specified cluster.
server-cluster port	Configures the specified IP, ARP entry to a given cluster and/or a multi-cast IP.
show server-cluster	Displays the clusters configured in the system.

MIB Objects

```
alaHAVlanClusterTable  
  alaHAVlanClusterId  
  alaHAVlanClusterName  
  alaHAVlanClusterAdminStatus  
  alaHAVlanClusterMode  
  alaHAVlanClusterRowStatus
```

server-cluster vlan

Configures a VLAN assignment for the specified cluster. This command is used to assign VLANs to an L2 cluster.

```
server-cluster cluster-id vlan vlan_id
```

Syntax Definitions

<i>cluster-id</i>	The numerical identifier of an existing server cluster.
<i>vlan_id</i>	The VLAN identifier to assign to the cluster. The valid range is 1–4094.

Defaults

NA

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- If the specified VLAN ID does not exist in the switch configuration, the cluster will remain operationally disabled.
- Modifying the existing VLAN assignment for a cluster is only allowed when the cluster is administratively disabled.

Examples

```
-> server-cluster 1 vlan 10  
-> server-cluster 5 vlan 10  
-> server-cluster 6 mac-address 00 :11 :22 :33 :44 :55
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster ip	Configures the specified IP, ARP entry to a given cluster.
server-cluster port	Configures the specified IP, ARP entry to a given cluster and/or a multi-cast IP.
show server-cluster	Displays the clusters configured in the system.
show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
alaHAVlanClusterTable  
  alaHAVlanClusterId  
  alaHAVlanClusterVlan  
  alaHAVlanClusterMacAddress  
  alaHAVlanClusterRowStatus
```

server-cluster mac-address

Configures a MAC address assignment for the specified cluster. This command is used to assign a MAC address to an L2 cluster.

server-cluster *cluster-id* **mac-address** *mac-address*

Syntax Definitions

cluster-id The numerical identifier of an existing server cluster.

mac-address The MAC address of the cluster.

Defaults

NA

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- Modifying the existing MAC address assignment for a cluster is only allowed when the cluster is administratively disabled.
- The MAC address that is assigned to a cluster can be a unicast, L2 multicast, or IP multicast address. However reserved multicast MAC addresses cannot be assigned to the cluster.

Examples

```
-> server-cluster 1 vlan 10 mac-address 00 :11 :22 :33 :44
-> server-cluster 5 vlan 10
-> server-cluster 5 mac-address 01:
-> server-cluster 6 mac-address 00 :11 :22 :33 :44 :55
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster ip	Configures the specified IP, ARP entry to a given cluster.
server-cluster port	Configures the port or linkagg to be assigned to a specific cluster.
show server-cluster	Displays the clusters configured in the system.
show mac-learning	Displays Source Learning MAC Address Table information.

MIB Objects

```
alaHAVlanClusterTable  
  alaHAVlanClusterId  
  alaHAVlanClusterVlan  
  alaHAVlanClusterMacAddress  
  alaHAVlanClusterRowStatus
```

server-cluster ip

Configures an IP address and ARP entry for the specified cluster. This command is used to assign an IP address to an L3 cluster.

```
server-cluster cluster-id ip ip-address [ mac-address {static mac-address | dynamic}]
```

Syntax Definitions

<i>cluster-id</i>	The numerical identifier of an existing server cluster.
<i>ip-address</i>	The unicast IP address to assign to the cluster.
<i>mac-address</i>	The MAC address for the static ARP entry.
dynamic	Dynamically resolve the ARP entry for the cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- A cluster can be assigned an IP address an ARP entry MAC address. Each cluster should have a unique IP address.
- Reserved MAC address cannot be configured as an ARP.
- Modifying the existing IP address parameters for a cluster is only allowed when the cluster is administratively disabled.

Examples

```
-> server-cluster 1 ip 10.135.33.203 mac-address static 00 :11 :22 :33 :44
-> server-cluster 3 ip 10.135.33.205 mac-address dynamic
-> server-cluster 5 ip 10.135.33.207
-> server-cluster 6 mac-address dynamic
-> server-cluster 7 mac-address static 00 :11 :22 :33 :44
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster mac-address	Configures a MAC address of the specified cluster.
server-cluster port	Configures the port or linkagg to be assigned to a specific cluster.
show server-cluster	Displays the clusters configured in the system.

MIB Objects

```
alaHAVlanClusterTable  
  alaHAVlanClusterId  
  alaHAVlanClusterIfIndex  
  alaHAVlanClusterInetAddressType  
  alaHAVlanClusterInetAddress  
  alaHAVlanClusterMacAddressType  
  alaHAVlanClusterMacAddress  
  alaHAVlanClusterMulticastStatus  
  alaHAVlanClusterMulticastInetAddressType  
  alaHAVlanClusterMulticastInetAddress  
  alaHAVlanClusterRowStatus
```

server-cluster igmp mode

Configures the IGMP mode status for specified cluster.

```
server-cluster cluster-id igmp-mode {enable | disable}
```

Syntax Definitions

<i>cluster-id</i>	The numerical identifier of an existing server cluster.
enable	Enables IGMP mode for cluster ports.
disable	Disables IGMP mode for cluster ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- When the IGMP mode is enabled for the cluster, the port list is dynamically learned using the IGMP protocol for the configured IP multicast address.
- For HA VLAN IGMP to work, IGMP must be enabled globally on the switch using the command **ip multicast admin-state enable** command.

Examples

```
-> server-cluster 4 igmp-mode enable  
-> server-cluster 4 igmp-mode disable
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster ip	Configures the specified IP, ARP entry to a given cluster.
show server-cluster	Displays the clusters configured in the system.

MIB Objects

alaHAVlanClusterTable

- alaHAVlanClusterId
- alaHAVlanClusterIfIndex
- alaHAVlanClusterInetAddressType
- alaHAVlanClusterInetAddress
- alaHAVlanClusterMacAddressType
- alaHAVlanClusterMacAddress
- alaHAVlanClusterMulticastStatus
- alaHAVlanClusterMulticastInetAddressType
- alaHAVlanClusterMulticastInetAddress
- alaHAVlanClusterRowStatus

server-cluster ip-multicast

Configures a multicast IP address for the specified cluster. This command configures an IP multicast address for an L3 cluster.

```
server-cluster cluster-id ip-multicast ipm-address
```

Syntax Definitions

<i>cluster-id</i>	The numerical identifier of an existing server cluster.
<i>ipm-address</i>	The multicast IP address to assign to the cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- A cluster can be assigned an IP address an ARP entry MAC address. Each cluster should have a unique IP-address. IP address is configurable only for L3 clusters
- Cluster parameters like IP, multicast IP and MAC address can be modified only when the cluster admin status is disabled.

Examples

```
-> server-cluster 2 ip-multicast 226.0.0.12  
-> server-cluster 4 ip-multicast 226.0.0.14
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster	Configures cluster parameters to create or modify a cluster ID.
show server-cluster	Displays the clusters configured in the system.

MIB Objects

alaHAVlanClusterTable

- alaHAVlanClusterId
- alaHAVlanClusterIfIndex
- alaHAVlanClusterInetAddressType
- alaHAVlanClusterInetAddress
- alaHAVlanClusterMacAddressType
- alaHAVlanClusterMacAddress
- alaHAVlanClusterMulticastStatus
- alaHAVlanClusterMulticastInetAddressType
- alaHAVlanClusterMulticastInetAddress
- alaHAVlanClusterRowStatus

server-cluster port

Configures a port assignment for the port list of the specified cluster.

```
server-cluster cluster-id port {slot/port[-port2] | all}
```

```
no server-cluster cluster-id port {slot/port[-port2] | all}
```

Syntax Definitions

<i>cluster-id</i>	The numerical identifier of an existing server cluster.
<i>slot/port</i>	The slot and port number to assign to the cluster port list. Use a hyphen to specify a range of ports (1/15-20).
all	Assigns all of the ports that belong to the associated VLAN and NOT all ports on the NI. This parameter applies only to L3 clusters.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- Use the **no** form of this command to remove a port from the specified cluster port list.
- The cluster ID specified with this command must already exist in the switch configuration.
- Using a port list is not valid for a cluster operating with IGMP mode enabled.
- The **all** parameter does not apply to L2 clusters.

Examples

```
-> server-cluster 1 port 1/21
-> server-cluster 2 port 1/21-23
-> server-cluster 5 port all
-> no server-cluster 1 port 1/21
-> no server-cluster 2 port 1/21-23
-> no server-cluster 3 port all
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster	Configures cluster parameters to create or modify a cluster ID.
show server-cluster	Displays the clusters configured in the system.
show mac-learning	Displays Source Learning MAC Address table information.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
alaHAVlanClusterPortTable  
  alaHAVlanClusterId  
  alaHAVlanClusterPortIfIndex  
  alaHAVlanClusterPortRowStatus
```

server-cluster linkagg

Configures a link aggregate assignment for the port list of the specified cluster.

```
server-cluster cluster-id linkagg agg_id[-agg_id2]
```

```
no server-cluster cluster-id linkagg agg_id[-agg_id2]
```

Syntax Definitions

<i>cluster-id</i>	The numerical identifier of an existing server cluster.
<i>agg_id</i> [- <i>agg_id2</i>]	The link aggregate ID number to assign to the cluster port list. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- Use the **no** form of this command to remove a link aggregate ID from the specified cluster port list.
- The cluster ID and link aggregate ID specified with this command must already exist in the switch configuration.
- Using a port list is not valid for a cluster operating with IGMP mode enabled.

Examples

```
-> server-cluster 3 linkagg 1  
-> server-cluster 4 linkagg 1-3  
-> no server-cluster 3 linkagg 1
```

Release History

Release 7.2.1; command was introduced.

Related Commands

server-cluster	Configures cluster parameters to create or modify a cluster ID.
show server-cluster	Displays the clusters configured in the system.
show mac-learning	Displays Source Learning MAC Address table information.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
alaHAVlanClusterPortTable  
  alaHAVlanClusterId  
  alaHAVlanClusterPortIfIndex  
  alaHAVlanClusterPortRowStatus
```

show server-cluster

Displays the cluster configuration information for the switch. If the cluster configuration is set up to run over a Multi-Chassis Link Aggregation (MCLAG) configuration, this command also provides the status of the MCLAG link for the specified cluster.

show server-cluster [*cluster-id* [**port**]]

Syntax Definitions

cluster-id The numerical identifier of an existing server cluster.

port Displays the ports and/or link aggregates assigned to a specific cluster.

Defaults

Displays a list of all server clusters configured for the switch.

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- Specify a cluster ID with this command to display information for a single cluster.
- Use the **port** parameter with the *cluster-id* parameter to display information about the ports assigned to the specified cluster.
- An asterisk (*) is displayed to indicate invalid cases, as shown in the command example.

Examples

```
-> show server-cluster
```

```
Legend: * = not valid
```

Cluster	Mode	Vlan	Mac Address	Ip Address	IGMP Address	Name
* 10	L2	100	01:10:11:22:33:44	-	-	cluster1
11	L2	100	01:10:11:22:33:44	-	-	cluster2
12	L2	100	01:10:11:22:33:44	-	-	-
13	L3	-	01:12:11:22:33:44	10.135.33.203	-	-
* 14	L3	-	01:12:11:22:33:45	10.135.33.203	-	-
15	L3	-	01:00:5e:00:00:44	10.135.33.203	225.0.1.2	cluster-igmp

```
-> show server-cluster 10 port
```

```
Legend: * = not valid
```

Cluster	Port	Port Type
* 10	1/3	Static
10	1/21	Static
* 10	0/2	Static

```
-> show server-cluster 11 port
Legend: * = not valid
Cluster  Port          Port Type
-----+-----+-----
10       1/3                 Dynamic
10       1/21                Dynamic
10       0/2                 Dynamic
```

output definitions

Cluster	The numerical identifier of a cluster.
Mode	Displays the cluster mode as L2 or L3 .
Vlan	Displays the VLAN identifier of the cluster.
MAC-Address	The MAC address associated with the cluster.
IP Address	The IP address associated with the cluster.
IGMP Address	The IGMP address associated with the cluster.
IGMP-Mode	Displays the status of IGMP-mode, Enabled or Disabled .
Name	The name representing the cluster.
Port	Displays the port list of the cluster.
Port Type	Displays the port type, Static or Dynamic .

```
-> show server-cluster 1
Cluster Id : 1,
Cluster Name : L2-cluster,
Cluster Mode : L2,
Cluster Mac-Address : 01:10:11:22:33:44,
Cluster Vlan : 12,
Administrative State: Enabled,
Operational State : Disabled,
Operational Flag : VPA is not forwarding
Multi-Chassis Status           : OutOfSync,
Multi-Chassis OutOfSync Reason  : Multi-Chassis Down,
VFL Status                     : Not-used
```

```
-> show server-cluster 2
Cluster Id : 2,
Cluster Name : -,
Cluster Mode : L3,
Cluster IP : 10.135.33.203,
Cluster Mac-Address : 01:10:11:22:33:44,
Cluster Mac Type : Dynamic,
IGMP-Mode : Disabled,
Cluster Multicast IP: -,
Administrative State: Enabled,
Operational State : Enabled,
Operational Flag : -,
Multi-Chassis Status           : OutOfSync,
Multi-Chassis OutOfSync Reason  : Synch In Progress,
VFL Status                     : Not-used
```

```

-> show server-cluster 3
  Cluster Id       : 3,
  Cluster Name     : L3-cluster,
  Cluster Mode     : L3,
  Cluster IP       : 10.135.33.203,
  Cluster Mac Type : Dynamic,
  Cluster Mac-Address : 01:00:5e:00:11:22,
  IGMP-Mode       : Enabled,
  Cluster Multicast IP: 225.0.1.2,
  Administrative State: Disabled,
  Operational State : Disabled,
  Operational Flag  : No IGMP reports received
Multi-Chassis Status      : InSync,
Multi-Chassis OutOfSync Reason : -,
VFL Status                : Used

```

output definitions

Cluster ID	The numerical identifier of a cluster.
Cluster Name	The name representing the cluster.
Cluster Mode	Displays the cluster mode as L2 or L3 .
Cluster IP	The IP address associated with the cluster.
Cluster Mac Type	The type of cluster, Static or Dynamic .
Cluster Mac-Address	The MAC address associated with the cluster.
IGMP-mode	Specifies the status of IGMP-mode, Enabled or Disabled .
Cluster Multicast IP	The multicast IP address associated with the cluster.
Administrative State	Specifies the administrative status of the cluster, Enabled or Disabled .
Operational State	Specifies the operational status of the cluster, Enabled or Disabled .
Operational Flag	Specifies the reason the cluster is operationally down.
Multi-Chassis Status	Whether or not the HAVLAN configuration is consistent between two MCLAG peer switches (InSync or OutOfSync).
Multi-Chassis OutOfSync Reason	Indicates one of the following reasons the HAVLAN is out of sync between the two MCLAG peer switches: <ul style="list-style-type: none"> • Multi-Chassis Down • Cluster Operational State Down • Server Cluster Mode Mismatch • VLAN Mismatch • MAC Address Mismatch • IP Address Mismatch • ARP Type Mismatch • IGMP Status Mismatch • Multicast IP Address Mismatch • All-port Mode Not Supported • Sync In Progress • Non-VIP-VLAN Not Supported In L3 Mode
VFL Status	Indicates whether the MCLAG Virtual Fabric Link (VFL) is Used or Not-used for the cluster.

Release History

Release 7.2.1; command was introduced.

Release 7.2.1.R02: **Multi-Chassis Status, Multi-Chassis OutOfSync Reason, VFL Status** fields added.

Related Commands

show mac-learning	Displays Source Learning MAC Address Table information.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
alaHAVlanClusterPortTable
  alaHAVlanClusterId
  alaHAVlanClusterPortIfIndex
  alaHAVlanClusterPortRowStatus
alaHAVlanClusterTable
  alaHAVlanClusterId
  alaHAVlanClusterInetAddress
  alaHAVlanClusterMacAddressType
  alaHAVlanClusterMacAddress
  alaHAVlanClusterMulticastStatus
  alaHAVlanClusterMulticastInetAddress
  alaHAVlanClusterVlan
  alaHAVlanClusterName
  alaHAVlanClusterAdminStatus
  alaHAVlanClusterMode
  alaHAVlanClusterOperStatus
  alaHAVlanClusterOperStatusFlag
  alaHAVlanClusterMcmStatus
  alaHAVlanClusterMcmStatusFlag
  alaHAVlanClusterVflStatus
```

6 Distributed Spanning Tree Commands

The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the Alcatel-Lucent STP implementation distributes the Spanning Tree load between the primary management module and the network interface modules. 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), and 802.1Q 2005 (MSTP).
- 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.
- A *per-VLAN* Spanning Tree operating mode that 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:

Bridge commands	<ul style="list-style-type: none"> spantree mode spantree protocol spantree priority spantree hello-time spantree max-age spantree forward-delay spantree bpdu-switching spantree path-cost-mode spantree vlan admin-state spantree auto-vlan-containment show spantree show spantree cist show spantree msti show spantree vlan show spantree mode
Port commands	<ul style="list-style-type: none"> spantree cist spantree vlan spantree priority spantree cist path-cost spantree msti path-cost spantree vlan path-cost spantree cist mode spantree vlan mode spantree cist connection spantree vlan connection spantree cist admin-edge spantree vlan admin-edge spantree cist auto-edge spantree vlan auto-edge spantree cist restricted-role spantree vlan restricted-role spantree cist restricted-tcn spantree vlan restricted-tcn spantree cist txholdcount spantree vlan txholdcount show spantree ports show spantree cist ports show spantree msti ports show spantree vlan ports
MST region commands	<ul style="list-style-type: none"> spantree mst region name spantree mst region revision-level spantree mst region max-hops show spantree mst
MST instance commands	<ul style="list-style-type: none"> spantree msti spantree msti vlan show spantree msti vlan-map show spantree cist vlan-map show spantree map-msti
PVST+ commands	<ul style="list-style-type: none"> spantree pvst+compatibility

spantree mode

Selects the flat Spanning Tree or per-VLAN Spanning Tree operating mode for the switch. These modes are exclusive; however, it is not necessary to reboot the switch when the STP modes are changed.

spantree mode {flat | per-vlan}

Syntax Definitions

flat	One Spanning Tree instance per switch.
per-vlan	One Spanning Tree instance for each VLAN configured on a switch.

Defaults

By default, the Spanning Tree mode for the switch is set to per-VLAN.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The Multiple Spanning Tree Protocol (MSTP), as defined in the IEEE 802.1Q 2005 standard, is only supported on switches operating in the flat Spanning Tree mode.
- If standard STP or RSTP is used when the switch is running in the flat mode, a single STP instance is applied across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 connect to the same switch together, then STP blocks one of these ports.
- If MSTP is used when the switch is running in the flat mode, a single STP instance is applied to each Multiple Spanning Tree Instance (MSTI). Each MSTI represents a set of VLANs.
- Flat Spanning Tree mode supports fixed (untagged) and 802.1Q tagged ports in each VLAN. However, Bridge Protocol Data Units (BPDUs) are always untagged.
- If the per-VLAN mode is selected, a single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances. In essence, a VLAN is a virtual bridge that has its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max-age, and forward delay.
- When operating in per-VLAN mode, 802.1Q tagged ports participate in an 802.1Q Spanning Tree instance that allows the Spanning Tree to extend across tagged VLANs. As a result, a tagged port can participate in more than one Spanning Tree instance; one for each VLAN that the port carries.
- If a VLAN contains both fixed and tagged ports and the switch is operating in per-VLAN Spanning Tree mode, then a hybrid of the two Spanning Tree instances (single and 802.1Q) is applied. If a VLAN appears as a tag on a port, then the BPDU for that VLAN are also tagged. However, if a VLAN appears as the configured default VLAN for the port, then BPDU are not tagged and the single Spanning Tree instance applies.
- Regardless of which mode the switch is running in, it is possible to administratively disable the Spanning Tree status for an individual VLAN (see [Chapter 4, “VLAN Management Commands”](#)).

Note. Active ports associated with such a VLAN are excluded from any Spanning Tree calculations and remain in a forwarding state.

Examples

```
-> spantree mode flat
-> spantree mode per-vlan
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree protocol	Selects the Spanning Tree protocol for the specified instance.
spantree bpdu-switching	Enables the switching of Spanning Tree BPDU on a VLAN that has Spanning Tree disabled.
show spantree	Displays VLAN Spanning Tree parameter values.

MIB Objects

```
vStpTable
  vStpNumber
  vStpMode
```

spantree protocol

Configures the Spanning Tree protocol for the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance.

```
spantree [cist | vlan vlan_id] protocol {stp | rstp | mstp}
```

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
<i>vlan_id</i>	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
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. This protocol is not supported on a per-VLAN basis.

Defaults

By default, the Spanning Tree protocol is set to RSTP.

parameter	default
cist vlan <i>vlan_id</i>	cist

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the optional **cist** or **vlan** parameter is not specified with this command, the protocol is set for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active.

Note. 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 per-VLAN Spanning Tree mode.
- Deleting all existing MSTIs is required before changing the protocol from MSTP to STP or RSTP.

Note. 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. However, if the path cost mode was set to 32-bit prior to the protocol change, the path cost is *not* reset to the default value. See the [spantree path-cost-mode](#) command page for more information.

Examples

```
-> spantree protocol mstp
-> spantree cist protocol mstp
-> spantree vlan 5 protocol rstp
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.

MIB Objects

```
vStpInsTable
  vStpInsNumber
  vStpInsMode
  vStpInsProtocolSpecification
```

spantree vlan admin-state

Enables or disables the Spanning Tree status for a VLAN.

```
spantree vlan vlan_id [-vlan_id2] admin-state {enable | disable}
```

Syntax Definitions

<i>vlan_id</i> [- <i>vlan_id2</i>]	An existing VLAN ID number. Use a hyphen to specify a range of VLANs (10-15).
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 for a VLAN instance.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

VLAN Spanning Tree instances are only active when the switch is running in the per-VLAN mode. However, configuring the VLAN Spanning Tree status is allowed in both modes (per-VLAN and flat).

Examples

```
-> spantree vlan 850-900 admin-state enable
-> spantree vlan 720-750 admin-state disable
-> spantree vlan 500 admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

vlan	Creates a VLAN.
show vlan	Displays a list of existing VLANs.
show vlan members	Displays VLAN port assignments.

MIB Objects

```
vlanTable
  vlanNumber
  vlanAdmStatus
  vlanOperStatus
  vlanStatus
```

spantree 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.

spantree mst region name *name*

no spantree mst region name

Syntax Definitions

name An alphanumeric string. Use quotes around string if the name contains multiple words with spaces between them (for example “Alcatel-Lucent Marketing”).

Defaults

By default, the MST region name is left blank.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the MST region name.

Note. It is not necessary to specify the region name to remove it.

- To change the existing region, use this command with a string value that is different than the existing region 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

```
-> spantree mst region name SalesRegion
-> spantree mst region name "Alcatel-Lucent Marketing"
-> no spantree mst region name
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region revision-level	Defines the revision level for an MST region.
spantree mst region max-hops	Defines the maximum number of hops for the MST region.
spantree msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
spantree msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

vStpMstRegionTable
 vStpMstRegionNumber
 vStpMstRegionConfigName

spantree 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.

spantree mst region revision-level *rev_level*

Syntax Definitions

rev_level A numeric value that identifies the MST region revision level for the switch.

Defaults

By default, the MST revision level is set to zero.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

An MST region revision level can be assigned to the MST region 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, using the MSTP.

Examples

```
-> spantree mst region revision-level 1000
-> spantree mst region revision-level 2000
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region name	Defines the name for an MST region.
spantree mst region max-hops	Defines the maximum number of hops for the MST region.
spantree msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
spantree msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable
  vStpMstRegionNumber
  vStpMstRegionConfigRevisionLevel
```

spantree 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 assign the maximum number of hops a BPDU is allowed to traverse, before it is discarded and related information is aged out.

spantree mst region max-hops *max_hops*

Syntax Definitions

max_hops A numeric value that designates the maximum number of hops.

Defaults

By default, the maximum number of hops is set to 20.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The value configured with this command is a regional value that applies to all instances and 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

```
-> spantree mst region max-hops 40
```

Release History

Release 7.1.1; command introduced.

Related Commands

<code>spantree mst region name</code>	Defines the name for an MST region.
<code>spantree mst region revision-level</code>	Defines the revision level for an MST region.
<code>spantree msti</code>	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
<code>spantree msti vlan</code>	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstRegionTable  
  vStpMstRegionNumber  
  vStpMstRegionMaxHops
```

spantree 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.

spantree msti *msti_id* [**name** *name*]

no spantree msti *msti_id* [**name**]

Syntax Definitions

<i>msti_id</i>	A numeric MSTI ID number. A range of VLANs is associated to an MSTI ID number.
<i>name</i>	An alphanumeric string. Use quotes around string if the name contains multiple words with spaces between them (for example “Alcatel-Lucent Marketing”).

Defaults

By default, a flat mode Common and Internal Spanning Tree (CIST) instance always exists. The MSTI ID number for this instance is 0.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the MSTI from the switch configuration.
- Use the **no** form of this command along with the **name** parameter to remove the optional MSTI name from the specified instance. The instance itself is not removed; only the name.
- There is always one CIST per switch. Initially all VLANs are associated with the CIST instance.
- Creating an MSTI is allowed when the switch is operating in either the per-VLAN 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

```
-> spantree msti 10
-> spantree msti 20 name BldgOneST10
-> no spantree msti 20 name
-> no spantree msti 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region name	Defines the name for an MST region.
spantree mst region revision-level	Defines the revision level for an MST region.
spantree mst region max-hops	Defines the maximum number of hops for the MST region.
spantree msti vlan	Defines an association between a range of VLANs and a single MSTI.

MIB Objects

```
vStpMstInstanceTable  
  vStpMstInstanceNumber  
  vStpMstInstanceName  
  vStpMstInstanceVlanBitmapAddition  
  vStpMstInstanceVlanBitmapDeletion  
  vStpMstInstanceVlanBitmapState
```

spantree 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.

```
spantree msti msti_id vlan vlan_id[-vlan_id2]
```

```
no spantree msti msti_id vlan vlan_id[-vlan_id2]
```

Syntax Definitions

<i>msti_id</i>	A numeric MSTI identification number. A range of VLANs are associated to an MSTI ID number.
<i>vlan_id</i>	A VLAN ID number.
[<i>vlan_id2</i>]	The last VLAN ID in a range of VLAN IDs.

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 10K, 6900

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.
- To associate multiple VLANs in a single command, use a hyphen to specify a range of VLAN IDs and a space to separate multiple VLAN IDs and/or ranges (for example 100-115 122 135 200-210).
- Configuring an MSTI-to-VLAN mapping is allowed when the switch is operating in either the per-VLAN 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

```
-> spantree msti 10 vlan 100-115
-> spantree msti 20 vlan 122
-> no spantree msti 10 vlan 100-115
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mst region name	Defines the name for an MST region.
spantree mst region revision-level	Defines the revision level for an MST region.
spantree mst region max-hops	Defines the maximum number of hops for the MST region.
spantree msti	Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.

MIB Objects

```
vStpMstVlanAssignmentTable  
  vStpMstVlanAssignmentVlanNumber  
  vStpMstVlanAssignmentEntry  
  vStpMstVlanAssignmentMstiNumber
```

spantree priority

Configures the bridge priority value for the Common and Internal Spanning Tree (CIST) instance, a Multiple Spanning Tree Instance (MSTI), or a VLAN instance. This command is also used to configure the priority value for a port or link aggregate associated with the CIST, an MSTI, or a VLAN.

```
spantree [cist | msti msti_id | vlan vlan_id] [port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]]
priority priority
```

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
<i>msti_id</i>	An existing MSTI ID number. If MSTI 0 is specified, the priority applies to the CIST instance. This parameter is configurable in both modes (flat or per-VLAN) but only if the flat mode protocol is set to MSTP.
<i>vlan_id</i>	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
<i>priority</i>	A bridge or port priority value. The valid range for the bridge priority is 0–65535. The valid range for the port priority is 0–15. If MSTP is the active flat mode protocol, enter a value that is a multiple of 4096 (for example, 4096, 8192, 12288).

Defaults

- By default, the bridge priority value is set to 32768 for the CIST, an MSTI, and a VLAN instance.
- By default, the port or link aggregate priority value is set to 7.

parameter	default
cist msti <i>msti_id</i> vlan <i>vlan_id</i>	cist

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The bridge priority is used to determine which bridge the Spanning Tree algorithm designates as the root bridge. The port priority value is used to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.
- The lower the bridge or port priority number assigned, the higher the priority that is associated with the bridge or port.

- If none of the optional instance parameters (**cist**, **msti**, or **vlan**) or **port** and **linkagg** parameters are specified with this command, the bridge priority is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the **cist**, **msti**, and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified priority values are not applied unless the supporting mode (flat for CIST/MSTI or per-VLAN for a VLAN instance) is active.
- To configure the bridge priority with this command, specify the instance (**cist**, **msti**, or **vlan**) and the priority value; do not specify a port number or link aggregate ID.
- 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).
- When the protocol is changed to/from MSTP, the bridge priority for the flat mode CIST instance is reset to the default value.
- 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. In regards to the priority for an MSTI, only the four most significant bits are used.
- To configure the port priority with this command, specify the instance (**cist**, **msti**, or **vlan**), a port number or link aggregate ID that is associated with that instance, and the priority value.
- The port priority value configured with this command is only applied to the specified instance. 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.
- 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.

Examples

The following command examples set the bridge priority for the specified instance:

```
-> spantree priority 8192
-> spantree cist priority 8192
-> spantree vlan 2 priority 32679
-> spantree msti 1 priority 2500
ERROR: Valid bridge priority values are multiples of 4096: 0, 4096,
      8192, 12288, 16384 ... 61440
-> spantree msti 1 priority 8192
```

The following command examples set the port priority for the specified instance:

```
-> spantree port 1/10 priority 10
-> spantree cist port 1/10 priority 10
-> spantree cist linkagg 10 priority 1
-> spantree vlan 200 port 2/1 priority 15
-> spantree vlan 2 linkagg 5 priority 2
-> spantree msti 2 port 1/24 priority 5
-> spantree msti 3 linkagg 6-8 priority 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.
show spantree ports	Displays the Spanning Tree port configuration.

MIB Objects

```
vStpInsTable  
  vStpInsNumber  
  vStpInsMode  
  vStpInsPriority  
  vStpInsBridgeAddress
```

spantree hello-time

Configures the Spanning Tree hello time value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN 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.

```
spantree [cist | vlan vlan_id] hello-time seconds
```

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
<i>vlan_id</i>	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
<i>seconds</i>	Specifies the Hello time value in seconds. The valid range is 1–10.

Defaults

By default, the bridge hello time value is set to 2 seconds.

parameter	default
cist vlan <i>vlan_id</i>	cist

Platforms Supported

OmniSwitch 10K, 6900

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.
- If the optional **cist** or **vlan** parameter is not specified with this command, the hello time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the **cist** and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified hello time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.
- 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

```
-> spantree hello-time 5
-> spantree cist hello-time 5
-> spantree vlan 10 hello-time 3
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.

MIB Objects

```
vStpInsTable  
  vStpInsNumber  
  vStpInsMode  
  vStpInsBridgeHelloTime
```

spantree max-age

Configures the bridge maximum age time value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN mode VLAN instance. This value is the amount of time, in seconds, that the Spanning Tree Protocol information learned from the network on any port is retained. This information is discarded when it ages beyond the maximum age value.

spantree [**cist** | **vlan** *vlan_id*] **max-age** *seconds*

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
<i>vlan_id</i>	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
<i>seconds</i>	Max-age time in seconds. The valid range is 6–40.

Defaults

By default, the bridge maximum age time value is set to 20 seconds.

parameter	default
cist vlan <i>vlan_id</i>	cist

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A low maximum age time causes the Spanning Tree Algorithm to reconfigure more often.
- If the optional **cist** or **vlan** parameter is not specified with this command, the maximum age time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the **cist** and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified maximum age time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.
- Note that for Multiple Spanning Tree Instances (MSTI), the maximum age time value is inherited from the CIST instance and is not a configurable parameter.

Examples

```
-> spantree max-age 10
-> spantree cist max-age 10
-> spantree vlan 10 max-age 30
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

show spantree

Displays the Spanning Tree instance configuration.

MIB Objects

vStpInsTable

 vStpInsNumber

 vStpInsBridgeMaxAge

spantree forward-delay

Configures the bridge forward delay time for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN 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.

spantree [**cist** | **vlan** *vlan_id*] **forward-delay** *seconds*

Syntax Definitions

cist	The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
<i>vlan_id</i>	An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
<i>seconds</i>	Forward delay time, in seconds. The valid range is 4–30.

Defaults

By default, the bridge forward delay time value is set to 15 seconds.

parameter	default
cist vlan <i>vlan_id</i>	cist

Platforms Supported

OmniSwitch 10K, 6900

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.
- If the optional **cist** or **vlan** parameter is not specified with this command, the forward delay time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the **cist** and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified forward delay time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.
- 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

```
-> spantree forward-delay 30
-> spantree cist forward-delay 30
-> spantree vlan 5 forward-delay 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
show spantree	Displays the Spanning Tree instance configuration.

MIB Objects

```
vStpInsTable
  vStpInsNumber
  vStpInsMode
  vStpInsBridgeForwardDelay
```

spantree bpdu-switching

Enables or disables the switching of Spanning Tree BPDU for VLAN and CIST instances if the switch is running in the per-VLAN mode.

```
spantree {vlan vlan_id | cist} bpdu-switching {enable | disable}
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
enable	Enables BPDU switching for the specified instance.
disable	Disables BPDU switching for the specified instance.

Defaults

By default, BPDU switching is disabled for VLAN or CIST instance.

Platforms Supported

OmniSwitch 10K, 6900

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.
- Use the **vlan** parameter along with the *vlan_id* to enable or disable BPDU switching for a particular VLAN.
- Use the **cist** parameter to enable or disable BPDU switching for the CIST instance.

Examples

```
-> spantree mode flat
-> spantree bpdu-switching enable
-> spantree bpdu-switching disable
-> spantree cist bpdu-switching enable
-> spantree cist bpdu-switching disable

-> spantree mode per-vlan
-> spantree vlan 10 bpdu-switching enable
-> spantree vlan 10 bpdu-switching disable
```

Release History

Release 7.1.1; command introduced.

Related Commands**vlan members untagged**

Enables or disables Spanning Tree instance for the specified VLAN.

show spantree

Displays VLAN Spanning Tree parameter values.

MIB Objects

vStpInsTable

vStpInsBpduSwitching

spantree 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.

spantree 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 10K, 6900

Usage Guidelines

- All path cost values, except those for MSTIs, are reset to the default path cost value when this mode is changed.
- When connecting a switch running in the 32-bit path cost mode to a switch running in the 16-bit mode, the 32-bit switch has a higher path cost value and thus an inferior path cost to the 16-bit switch. To avoid this, use the **spantree 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

```
-> spantree path-cost-mode 32bit
-> spantree path-cost-mode auto
```

Release History

Release 7.1.1; command introduced.

Related Commands

[spantree protocol](#) Configures the protocol for the flat mode CIST instance or a per-VLAN mode VLAN instance.

MIB Objects

vStpBridge

vStpPathCostMode

spantree pvst+compatibility

Enables or disables PVST+ mode on the switch, port or link aggregate enabling them to operate with Cisco switches.

```
spantree pvst+compatibility {port slot/port} | linkagg linkagg_id} {enable | disable | auto}
```

Syntax Definitions

enable	Enables the PVST+ mode.
disable	Disables the PVST+ mode.
auto	IEEE BPDUs are used until a PVST+ BPDU is detected.
<i>slot/port</i>	Specifies the slot number for the module and the physical port number or a range of ports on that module (for example, 3/1 specifies port 1 on slot 3).
<i>linkagg_id</i>	Link aggregate ID number.

Defaults

PVST+ is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- In order to handle PVST+ mode, the ports must be configured in per-VLAN mode.
- Specify **pvst+compatibility enable** to enable all the ports on the switch to handle PVST+ BPDUs.
- Initially, a port sends or receive IEEE BPDUs. Once a PVST+ BPDU is received, the port sends and receives only PVST+ BPDUs for tagged VLANs and IEEE BPDUs for default VLANs.

Examples

```
-> spantree pvst+compatibility enable
-> spantree pvst+compatibility disable
-> spantree port 1/3 pvst+compatibility enable
-> spantree port 2/2 pvst+compatibility auto
-> spantree linkagg 2 pvst+compatibility enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree	Displays Spanning Tree bridge information for all flat mode Common and Internal Spanning Tree (CIST) instance and per-VLAN mode VLAN instance.
show spantree ports	Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance or a per-VLAN mode VLAN instance.
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).

MIB Objects

vStpPortConfigPVST
vStpPortConfigStatePVST
vStpBridgeModePVST

spantree 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.

```
spantree [msti msti_id] auto-vlan-containment {enable | disable}
```

Syntax Definitions

<i>msti_id</i>	An existing MSTI ID number. A range of VLANs are associated to an MSTI ID number.
enable	Enables automatic VLAN containment.
disable	Disables automatic VLAN containment.

Defaults

By default, automatic VLAN containment is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The AVC feature is not active for any MSTI until it is globally enabled. To globally enable this feature, use the **spantree 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, specify the *msti_id* for the instance and use the **disable** form of this command.
- 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. However, if the port path cost is administratively set to zero, then the path cost is reset to the default value.
- Note that when AVC is disabled, a port assigned to a VLAN that is 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

```
-> spantree auto-vlan-containment enable
-> spantree auto-vlan-containment disable
-> spantree msti 1 auto-vlan-containment disable
-> spantree msti 1 auto-vlan-containment enable
```


Release History

Release 7.1.1; command introduced.

Related Commands

[show spantree msti ports](#)

Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).

MIB Objects

vStpInsTable

 vStpInsAutoVlanContainment

vStpBridge

 vStpBridgeAutoVlanContainment

spantree cist

Enables or disables the Spanning Tree status on a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance.

```
spantree cist {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} {enable | disable}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id[-linkagg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
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 10K, 6900

Usage Guidelines

- This command only applies to the CIST instance regardless of which Spanning Tree operating mode (flat or per-VLAN) or protocol is active for the switch.
- If the switch is running in per-VLAN 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.
- When the Spanning Tree status is disabled on a port, the port is set to a forwarding state for the specified instance.
- 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

```
-> spantree cist port 4/1 enable
-> spantree cist port 4/2-5 disable
-> spantree cist linkagg 16 disable
-> spantree cist linkagg 22-26 enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree vlan

Configures the Spanning Tree status on a port or a link aggregate of ports for a VLAN instance.

MIB Objects

vStpInsPortTable

 vStpInsPortNumber

 vStpInsPortEnable

spantree vlan

Enables or disables the Spanning Tree status on a port or a link aggregate of ports for the specified VLAN instance.

```
spantree vlan vlan_id [-vlan2] {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} {enable | disable}
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
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 10K, 6900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which Spanning Tree operating mode (flat or per-VLAN) is active for 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 per-VLAN mode.
- 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 per-VLAN 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 when this occurs, ports will *not* bridge 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

```
-> spantree vlan 2 port 4/1 enable  
-> spantree vlan 2 port 4/2-5 disable
```

```
-> spantree vlan 3 linkagg 16 disable  
-> spantree vlan 3 linkagg 22-25 disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist	Configures the Spanning Tree status on a port or an aggregate of ports for the CIST instance when the switch is operating in either the per-VLAN or flat mode.
spantree vlan admin-state	Enables or disables Spanning Tree instance for the specified VLAN.
spantree bpdu-switching	Enables or disables the switching of Spanning Tree BPDU for all VLAN instances if the switch is running in the per-VLAN mode.

MIB Objects

```
vStpInsPortTable  
    vStpInsPortNumber  
    vStpInsPortEnable
```

spantree cist path-cost

Configures the Spanning Tree path cost value for a port or a link 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.

```
spantree cist {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} path-cost path_cost
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id[-linkagg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
<i>path_cost</i>	Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the port path cost value for the CIST instance regardless of which operating mode (flat or per-VLAN) or protocol is active for the switch.
- If the switch is running in per-VLAN 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 [spantree 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

Link Speed	Aggregate Size (number of links)	Default Path Cost Value
1 Gbps	N/A	3
10 Gbps	N/A	1

Examples

```
-> spantree cist port 4/1 path-cost 19
-> spantree cist port 4/2-5 path-cost 19
-> spantree cist linkagg 16 path-cost 12000
-> spantree cist linkagg 17-20 path-cost 12000
```

Release History

Release 7.1.1; command introduced.

Related Commands

[spantree mode](#)

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

[spantree path-cost-mode](#)

Selects a 32-bit or automatic path cost mode for the switch.

[spantree msti path-cost](#)

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for an MSTI.

[spantree vlan path-cost](#)

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for a VLAN instance.

MIB Objects

```
vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortPathCost
```

spantree msti path-cost

Configures the Spanning Tree path cost value for a port or a link 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.

```
spantree msti msti_id {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} path-cost path_cost
```

Syntax Definitions

<i>msti_id</i>	An existing MSTI ID number. If MSTI 0 is specified, the priority applies to the CIST instance.
<i>slot/port[-port2]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id[-linkagg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
<i>path_cost</i>	Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the specified MSTI regardless of which operating mode (flat or per-VLAN) is active for the switch. However, if MSTP is not the selected flat mode protocol, 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.
- 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 35000 for MSTI 3.
- If the switch is running in per-VLAN 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.
- 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

```
-> spantree msti 0 port 4/1 path-cost 35000
-> spantree msti 0 port 1/20-24 path-cost 12000
-> spantree msti 2 linkagg 10 path-cost 20000
-> spantree msti 2 linkagg 10-12 path-cost 65000
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist path-cost	Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the CIST instance.
spantree vlan path-cost	Configures the Spanning Tree path cost value for a port or a link aggregate of ports for a VLAN instance.

MIB Objects

```
vStpInsPortTable  
  vStpInsPortNumber  
  vStpInsPortPathCost
```

spantree vlan path-cost

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the specified 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.

```
spantree vlan vlan_id {port slot/port[-port2] / linkagg linkagg_id [-linkagg_id2]} path-cost path_cost
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
<i>path_cost</i>	Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

Defaults

By default, the path cost is set to zero.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for 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 per-VLAN 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 [spantree 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 IEEE 802.1S recommended default path cost values based on link speed are used:

Link Speed	IEEE 802.1S Recommended Value
10 MB	2,000,000
100 MB	200,000

Link Speed	IEEE 802.1D Recommended Value
1 GB	20,000
10 Gbps	2,000

- If a 16-bit path cost value is in use and the *path_cost* is set to zero, the following IEEE 802.1D recommended default path cost values 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

```
-> spantree vlan 200 port 4/1 path-cost 4
-> spantree vlan 200 port 4/2-5 path-cost 4
-> spantree vlan 300 linkagg 16 path-cost 200000
-> spantree vlan 500 linkagg 24-28 path-cost 20000
```

Release History

Release 7.1.1; command introduced.

Related Commands

[spantree mode](#)

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

[spantree cist path-cost](#)

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the CIST instance.

[spantree msti path-cost](#)

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for an MSTI.

MIB Objects

```
vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortPathCost
```

spantree cist mode

Configures manual mode (forwarding or blocking) or dynamic mode to manage the state of a port or a link 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.

spantree cist {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} mode {forwarding | dynamic | blocking}

Syntax Definitions

<i>slot/port[-port2]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id[-linkagg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
forwarding	Sets the port state to forwarding.
dynamic	Port state is determined by the Spanning Tree algorithm.
blocking	Sets the port state to blocking.

Defaults

By default, the port Spanning Tree mode is set to dynamic.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the port Spanning Tree mode for the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in per-VLAN 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.
- 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

```
-> spantree cist port 4/1 mode forwarding
-> spantree cist port 4/2-5 mode forwarding
-> spantree cist linkagg 10 mode blocking
-> spantree cist linkagg 15-20 mode forwarding
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree vlan mode

Configures the Spanning Tree mode for a port or a link aggregate of ports for the specified VLAN instance.

MIB Objects

vStpInsPortTable

 vStpInsPortNumber

 vStpInsPortManualMode

spantree vlan mode

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or a link aggregate of ports for the specified VLAN instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

spantree vlan *vlan_id* {**port** *slot/port*[-*port2*] | **linkagg** *linkagg_id* [-*linkagg_id2*]} **mode** {**dynamic** | **blocking** | **forwarding**}

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
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 10K, 6900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for 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 per-VLAN mode.
- 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

```
-> spantree vlan 255 port 4/1-4 mode forwarding
-> spantree vlan 355 port 1/24 mode dynamic
-> spantree vlan 450 linkagg 1 mode dynamic
-> spantree vlan 450 linkagg 1-5 mode dynamic
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree cist mode

Configures the Spanning Tree mode for a port or a link aggregate of ports for the CIST instance.

MIB Objects

vStpInsPortTable

 vStpInsPortNumber

 vStpInsPortManualMode

spantree cist connection

Configures the connection type for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

```
spantree cist {port slot/port [-port2] | linkagg linkagg_id [-linkagg_id2]} connection {noptp | ptp | autoptp}
```

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
noptp	Defines port connection type as no point to point link.
ptp	Defines port connection type as point to point link.
autoptp	Specifies that switch software automatically defines connection type as point-to-point or no point-to-point.

Defaults

By default, the link connection type is set to auto point-to-point.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the port connection type for the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in per-VLAN 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.
- 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 must run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point-to-point LAN segment.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point-to-point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

Examples

```
-> spantree cist port 7/24 connection noptp
-> spantree cist port 7/25-28 connection ptp
-> spantree cist linkagg 5-10 connection autoptp
-> spantree cist linkagg 5-10 connection autoptp
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the flat mode CIST instance.

MIB Objects

```
vStpInsPortTable  
  vStpInsPortNumber  
  vStpInsPortAdminConnectionType  
  vStpInsPortOperConnectionType
```

spantree vlan connection

Configures the connection type for a port or a link aggregate of ports for a VLAN instance.

```
spantree vlan vlan_id {port slot/port [-port2] / linkagg linkagg_id [-linkagg_id2]} connection {noptp | ptp | autoptp}
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>slot/port</i> [<i>-port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [<i>-linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
noptp	Defines port connection type as no point-to-point link.
ptp	Defines port connection type as point-to-point link.
autoptp	Specifies that switch software automatically defines connection type as point-to-point or no point-to-point <i>and</i> whether or not the port is an edge port.

Defaults

By default, the link connection type is set to auto point-to-point.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for 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 per-VLAN mode.
- 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 must run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point-to-point LAN segment.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

Examples

```
-> spantree vlan 255 port 7/24 connection noptp
-> spantree vlan 255 port 7/25-27 connection ptp
-> spantree vlan 255 linkagg 3 connection autoptp
-> spantree vlan 255 linkagg 3-7 connection autoptp
```

Release History

Release 7.1.1; command introduced.

Related Commands

[spantree mode](#)

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch

[spantree cist admin-edge](#)

Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.

[spantree cist auto-edge](#)

Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the flat mode CIST instance.

MIB Objects

vStpInsPortTable

 vStpInsPortNumber

 vStpInsPortAdminConnectionType

 vStpInsPortOperConnectionType

spantree cist admin-edge

Configures the administrative edge port status for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

```
spantree cist {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} admin-edge {enable | disable}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id[-linkagg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs
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 10K, 6900

Usage Guidelines

- This command only applies to the port connection type for the CIST instance regardless of which operating mode (flat or per-VLAN) is active on the switch.
- If the switch is running in the per-VLAN 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.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that connect to a host (PC, workstation, server, and so on) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point-to-point connection type.

Examples

```
-> spantree cist linkagg 15 admin-edge enable
-> spantree cist linkagg 4-10 admin-edge enable
-> spantree cist port 8/25 admin-edge disable
-> spantree cist port 2/2-5 admin-edge enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch
spantree vlan admin-edge	Configures the administrative edge port status for a port or a link aggregate of ports for a specific VLAN instance.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or a link aggregate of ports for the flat mode CIST instance.
spantree vlan auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or a link aggregate of ports for the specified per-VLAN mode VLAN instance.

MIB Objects

```
vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortAdminEdge
```

spantree vlan admin-edge

Configures the administrative edge port status for a port or a link aggregate of ports for a VLAN instance.

```
spantree vlan vlan_id {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} admin-edge {enable | disable}
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs
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 10K, 6900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for 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 per-VLAN Spanning Tree mode.
- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.
- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point to point connection type.

Examples

```
-> spantree vlan 4 linkagg 15 admin-edge enable
-> spantree vlan 5 linkagg 12-14 admin-edge enable
-> spantree vlan 255 port 8/23 admin-edge disable
-> spantree vlan 3 port 2/2-5 admin-edge enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or aggregate of ports for the flat mode CIST instance.
spantree vlan auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.

MIB Objects

```
vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortAdminEdge
```

spantree cist auto-edge

Configures whether or not Spanning Tree automatically determines the operational edge port status of a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

spantree cist {port *slot/port[-port2]* / linkagg *linkagg_id* [-*linkagg_id2*]} **auto-edge** {enable | disable}

Syntax Definitions

<i>slot/port[-port2]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs.
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.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the per-VLAN 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.
- 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 connection type of the port is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point to point connection type.

Examples

```
-> spantree cist linkagg 15 auto-edge enable
-> spantree cist linkagg 10-12 auto-edge disable
-> spantree cist port 8/23 auto-edge disable
-> spantree cist port 2/2-5 auto-edge enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch
spantree vlan auto-edge	Configures whether or not Spanning Tree determines the operational edge port status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree vlan admin-edge	Configures the administrative edge port status for a port or aggregate of ports for a specific VLAN instance.

MIB Objects

vStpInsPortTable
 vStpInsPortNumber
 vStpInsPortAutoEdge

spantree vlan auto-edge

Configures whether or not Spanning Tree determines the operational edge port status for a port or a link aggregate of ports for the specified per-VLAN mode VLAN instance.

spantree vlan *vlan_id* {**port** *slot/port*[-*port2*] / **linkagg** *linkagg_id* [-*linkagg_id2*]} **auto-edge** {**enable** | **disable**}

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs.
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 10K, 6900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for 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 per-VLAN Spanning Tree mode.
- 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 connection type of the port is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
- Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also 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 operationally reverts back to a no point to point connection type.

Examples

```
-> spantree vlan 255 port 8/23 auto-edge disable
-> spantree vlan 4 port 2/2-10 auto-edge enable
-> spantree vlan 100 linkagg 10 auto-edge disable
-> spantree vlan 200 linkagg 1-5 auto-edge enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist auto-edge	Configures whether or not Spanning Tree automatically determines the operational edge status of a port or aggregate of ports for the flat mode CIST instance.
spantree cist admin-edge	Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree vlan admin-edge	Configures the administrative edge port status for a port or aggregate of ports for a specific VLAN instance.

MIB Objects

```
vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortAutoEdge
```

spantree cist restricted-role

Configures the restricted role status for a port or a link aggregate of ports. Enabling this parameter blocks the port from becoming the Root Port, even if it is the most likely candidate for root. Once a root port is selected, the restricted port is selected as an Alternate Port.

```
spantree cist {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} restricted-role {enable | disable}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id[-linkagg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs
enable	Enables the restricted role status for the specified port.
disable	Disables the restricted role status for the specified port.

Defaults

By default, the restricted role status for the port is disabled.

Platforms Supported

OmniSwitch 10K, 6900

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.
- Enabling the restricted role status is used by network administrators to prevent bridges external to the core region of the network from influencing the Spanning Tree topology.
- Note that enabling the restricted role status for a port may impact connectivity within the network.

Examples

```
-> spantree cist linkagg 15-20 restricted-role enable
-> spantree cist port 8/23 restricted-role disable
-> spantree cist port 8/24-27 restricted-role disable
-> spantree cist linkagg 10 restricted-role disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree vlan restricted-role

Configures the restricted role status for a port or aggregate of ports for the per-VLAN mode VLAN instance.

MIB Objects

vStpInsPortTable

 vStpInsPortNumber

 vStpInsPortRestrictedRole

spantree vlan restricted-role

Configures the restricted role status for a port or a link aggregate of ports for the specified VLAN instance. Enabling this parameter blocks the port from becoming the Root Port, even if it is the most likely candidate for root. Once a Root Port is selected, the restricted port is selected as an Alternate Port.

```
spantree vlan vlan_id {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} restricted-role {enable | disable}
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs
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 restricted role status for the port is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Enabling the restricted role status is used by network administrators to prevent bridges external to the core region of the network from influencing the Spanning Tree topology.
- Note that enabling the restricted role status for a port may impact connectivity within the network.
- This command only applies to the VLAN instance specified by the VLAN ID regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified restricted role status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.

Examples

```
-> spantree vlan 3 linkagg 15 restricted-role enable
-> spantree vlan 255 port 8/23 restricted-role enable
-> spantree vlan 255 port 8/24-27 restricted-role enable
-> spantree vlan 255 linkagg 11-15 restricted-role enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree cist restricted-role

Configures the restricted role status for a port or aggregate of ports for the flat mode CIST instance.

MIB Objects

vStpInsPortTable

 vStpInsPortNumber

 vStpInsPortRestrictedRole

spantree cist restricted-tcn

Configures the restricted TCN status for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST). When this parameter is enabled, the port does not propagate topology changes and notifications to/from other ports.

```
spantree cist {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} restricted-tcn {enable | disable}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id[-linkagg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs.
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 10K, 6900

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 only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the per-VLAN 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.

Examples

```
-> spantree cist linkagg 15 restricted-tcn enable
-> spantree cist port 8/23 restricted-tcn disable
-> spantree cist port 2/2-4 restricted-tcn enable
-> spantree cist linkagg 10-14 restricted-tcn disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree vlan restricted-tcn

Configures the restricted TCN status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.

MIB Objects

vStpInsPortTable

 vStpInsPortNumber

 vStpInsPortRestrictedTcn

spantree vlan restricted-tcn

Configures the restricted TCN status for a port or a link aggregate of ports for the specified VLAN instance. When this parameter is enabled, the port does not propagate topology changes and notifications to/from other ports.

```
spantree vlan vlan_id {port slot/port [-port2] / linkagg linkagg_id [-linkagg_id2]} restricted-tcn {enable | disable}
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>slot/port</i> [- <i>port2</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>linkagg_id</i> [- <i>linkagg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs.
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 10K, 6900

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 only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for 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 per-VLAN Spanning Tree mode.

Examples

```
-> spantree vlan 2 linkagg 15 restricted-tcn enable
-> spantree vlan 2 linkagg 16-20 restricted-tcn enable
-> spantree vlan 255 port 8/23 restricted-tcn disable
-> spantree vlan 255 port 8/24-27 restricted-tcn disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

[spantree mode](#)

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

[spantree cist restricted-tcn](#)

Configures the restricted TCN status for a port or aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

MIB Objects

vStpInsPortTable

 vStpInsPortNumber

 vStpInsPortRestrictedTcn

spantree 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.

spantree cist txholdcount *value*

Syntax Definitions

value A numeric value that controls the transmission of BPDU through the port. The valid range is 1–10.

Defaults

By default, the **txholdcount** value is set to 3.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the per-VLAN 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.

Examples

```
-> spantree cist txholdcount 5
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree vlan txholdcount Configures the BPDU transmission rate limit for the specified VLAN instance.

MIB Objects

vStpInsTable

vStpInsBridgeTxHoldCount

spantree vlan txholdcount

This command is used to rate limit the transmission of BPDU through a given port for the VLAN instance.

```
spantree vlan vlan_id txholdcount {value}
```

Syntax Definitions

<i>vlan_id</i>	An existing VLAN ID number.
<i>value</i>	A numeric value that controls the transmission of BPDU through the port. The valid range is 1–10.

Defaults

By default, the **txholdcount** value is set to 3.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for 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 per-VLAN Spanning Tree mode.

Examples

```
-> spantree vlan 3 txholdcount 6
```

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode	Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
spantree cist txholdcount	Configures the BPDU transmission rate limit for the CIST instance.

MIB Objects

```
vStpInsTable  
  vStpInsBridgeTxHoldCount
```

show spantree

Displays Spanning Tree bridge information for the flat mode Common and Internal Spanning Tree (CIST) instance or the per-VLAN mode VLAN instances.

show spantree

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the switch is operating in the per-VLAN mode, this command displays a list of VLAN instances.
- If the switch is operating in the flat mode and the protocol is STP or RSTP, this command displays the single flat mode instance.
- If the switch is operating in the flat mode and the protocol is set to MSTP, this command displays a list of MSTIs, including MSTI 0 (also known as the CIST).

Examples

```
-> spantree mode flat
-> spantree protocol rstp
-> show spantree
```

```
Spanning Tree Path Cost Mode : 32 BIT
Bridge STP Status Protocol Priority(Prio:SysID)
-----+-----+-----+-----
      1      ON      RSTP   32768 (0x8000:0x0000)
```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (32 BIT or AUTO). Configured through the spantree 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.
STP 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 spantree protocol command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the spantree priority command.

```

-> spantree mode flat
-> spantree 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 spantree path-cost-mode command.
Msti	The Multiple Spanning Tree Instance (MSTI) instance number. Configured through the spantree msti command. Note that MSTI 0 also represents the CIST instance that is always present on the switch.
STP Status	The Spanning Tree state for the MSTI (ON or OFF).
Protocol	The Spanning Tree protocol applied to this instance. Configured through the spantree protocol command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the spantree priority command.

```

-> spantree mode per-vlan
-> 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)

```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (32 BIT or AUTO) Configured through the spantree path-cost-mode command.
Spanning Tree PVST+ Mode	Indicates whether the PVST + status is enabled or disabled. Configured through the spantree pvst+compatibility 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 spantree vlan admin-state command.

output definitions (continued)

Protocol	The Spanning Tree protocol applied to this instance (STP or RSTP). Configured through the spantree protocol command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the spantree priority command.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree cist	Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree msti	Displays the Spanning Tree bridge configuration for an MSTI regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree vlan	Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch.

MIB Objects

```
vStpInsTable
  vStpInsNumber
  vStpInsProtocolSpecification
  vStpInsMode
  vStpInsPriority
  vStpInsBridgeAddress
  vStpInsDesignatedRoot
  vStpInsRootCost
  vStpInsRootPortNumber
  vStpInsNextBestRootCost
  vStpInsNextBestRootPortNumber
  vStpInsBridgeTxHoldCount
  vStpInsTopChanges
  vStpInsTimeSinceTopologyChange
  vStpInsMaxAge
  vStpInsForwardDelay
  vStpInsHelloTime
```

show spantree cist

Displays the Spanning Tree bridge configuration for the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guideline

This command displays Spanning Tree bridge information for the flat mode CIST instance regardless of which mode (per-VLAN or flat) is active on the switch. Note that minimal information is displayed when this command is used in the per-VLAN mode, as the CIST is not active in this mode. See second example below.

Examples

```
-> spantree mode flat
-> show spantree cist
Spanning Tree Parameters for Cist
  Spanning Tree Status :                ON,
  Protocol              :                IEEE Multiple STP,
  mode                  :                FLAT (Single STP),
  Auto-Vlan-Containment:                Enabled ,
  Priority               :                32768 (0x8000),
  Bridge ID             :                8000-00:d0:95:01:39:2c,
  CST Designated Root  :                8000-00:d0:95:01:39:2c,
  Cost to CST Root     :                0,
  Next CST Best Cost   :                0,
  Designated Root     :                8000-00:d0:95:01:39:2c,
  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,
  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 =                20,
```

```

    System Hello Time      =    10
    BPDU Switching Enabled

-> spantree mode per-vlan
-> show spantree cist

Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters for Flat Mode
Spanning Tree Status :          ON,
Protocol              :          IEEE Rapid STP,
Priority               :          32768 (0x8000),
TxHoldCount           :          5,
System Max Age (seconds) =          10,
System Forward Delay (seconds) =          10,
System Hello Time (seconds) =          5

```

output definitions

Spanning Tree 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 spantree protocol command.
Mode	The Spanning Tree operating mode for the switch (per-vlan or flat). Configured through the spantree mode command.
Auto-Vlan-Containment	The auto VLAN containment status for the instance (Enabled or Disabled). AVC prevents a port that has no VLANs mapped to a Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Configured through the spantree auto-vlan-containment command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the spantree 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.

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).
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the spantree max-age command.
Forward Delay	The amount of time (in seconds) that a port remains in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the spantree 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 spantree 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 7.1.1; command introduced.

Related Commands

show spantree	Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.
show spantree msti	Displays the Spanning Tree bridge configuration for an MSTI regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree vlan	Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN 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.

Defaults

By default, displays information for all MSTIs.

Platforms Supported

OmniSwitch 10K, 6900

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 command displays Spanning Tree bridge information for an MSTI regardless of which mode (per-VLAN or flat) is active for the switch.
- Note that minimal information is displayed when this command is used in the per-VLAN mode, as MSTIs are not active in this mode. In addition, this command fails if MSTP is not the selected flat mode protocol.
- Note that MSTI 0 also represents the CIST instance that is always present on the switch. To view the CIST instance using this command, specify zero (0) for the *msti_id* number.

Examples

```
-> spantree mode flat
-> spantree 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

```

-> spantree mode per-vlan

-> 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 !! (per-vlan mode)
INACTIVE Spanning Tree Parameters for Cist
  Spanning Tree Status :          ON,
  Protocol              :          IEEE Multiple STP,
  Priority               :          32768 (0x8000),
  TxHoldCount          :           5,
  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 !! (per-vlan mode)
INACTIVE Spanning Tree Parameters for Msti 2
  Spanning Tree Status :          ON,
  Protocol              :          IEEE Multiple STP,
  Priority               :          32770 (0x8002),
  TxHoldCount          :           5,
  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 spantree path-cost-mode command.
Msti	The Multiple Spanning Tree Instance (MSTI) number. MSTI 0 represents the CIST. Configured through the spantree 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 spantree protocol command.
Mode	The Spanning Tree operating mode for the switch (per-vlan or flat). Configured through the spantree mode command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the spantree 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.

output definitions (continued)

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.
TxHoldCount	The count to limit the transmission of BPDU through the port.
Topology Changes	The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.
Topology age	The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (hh:mm:ss or dd days and hh:mm:ss).
Max Age	The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. MSTIs inherit this value from the CIST instance.
Forward Delay	The amount of time (in seconds) that a port remains in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. MSTIs inherit this value from the CIST instance.
Hello Time	The amount of time (in seconds) between the transmission of Configuration BPDUs on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. MSTIs inherit this value from the CIST instance.
System Max Age	The Max Age value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.
System Forward Delay	The Forward Delay value for the root bridge.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree	Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.
show spantree cist	Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree vlan	Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN 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 vlan

Displays Spanning Tree bridge information for a per-VLAN mode VLAN instance.

```
show spantree vlan [vlan_id]
```

Syntax Definitions

vlan_id An existing VLAN ID number.

Defaults

By default, displays information for all VLAN instances.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If a *vlan_id* number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all VLAN instances.
- Specify a *vlan_id* number with this command to display Spanning Tree bridge information for a specific VLAN instance.
- This command displays Spanning Tree bridge information for a VLAN instance regardless of which mode (per-VLAN 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

```
-> spantree mode per-vlan
-> show spantree vlan
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 vlan 6
Spanning Tree Parameters for Vlan 6
Spanning Tree Status :          ON,
Protocol              :          IEEE STP,
mode                  : Per VLAN (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

-> spantree mode flat
-> show spantree vlan 1
Single/Multiple Spanning Tree is enforced !! (flat mode)
INACTIVE Spanning Tree Parameters for Vlan 1
Spanning Tree Status : ON,
Protocol              : IEEE Rapid STP,
Priority               : 32768 (0x8000),
TxHoldCount           : 5,
System Max Age (seconds) = 20,
System Forward Delay (seconds) = 5,
System Hello Time (seconds) = 5

```

output definitions

Spanning Tree Path Cost Mode	The Spanning Tree path cost mode for the switch (32 BIT or AUTO). Configured through the spantree 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 spantree protocol command.
Mode	The Spanning Tree operating mode for the switch (per-vlan or flat). Configured through the spantree mode command.
Priority	The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the spantree 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.

output definitions (continued)

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 spantree max-age command.
Forward Delay	The amount of time (in seconds) that a port remains in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the spantree 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 spantree 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 7.1.1; command introduced.

Related Commands

show spantree	Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.
show spantree cist	Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.
show spantree msti	Displays the Spanning Tree bridge information for an MSTI when the switch is operating in the per-VLAN 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
```

show spantree ports

Displays Spanning Tree port information.

show spantree ports [**forwarding** | **blocking** | **active** | **configured**]

Syntax Definitions

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.

Defaults

parameter	default
forwarding blocking active configured	all ports

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the switch is operating in the per-VLAN mode, this command displays port information for the VLAN instances.
- If the switch is operating in the flat mode and the protocol is STP or RSTP, this command displays port information for the single flat mode instance.
- If the switch is operating in the flat mode and the protocol is set to MSTP, this command displays port information for the MSTIs, including MSTI 0 (also known as the CIST).

Examples

```
-> spantree mode flat
-> spantree protocol rstp
-> 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

```

```
-> spantree protocol mstp
```

```
-> show spantree ports
```

Msti	Port	Oper Status	Path Cost	Role
0	1/1	DIS	0	DIS
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

```
-> spantree mode per-vlan
```

```
-> show spantree ports
```

Vlan	Port	Oper Status	Path Cost	Role	Notes
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	DI	

output definitions

Bridge, Msti, or Vlan

The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol in the flat mode. The MSTI number when MSTP is the active protocol in the flat mode. The VLAN ID number when STP or RSTP is the active protocol in the per-VLAN mode.

Port

The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).

Oper Status

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 spantree msti path-cost or spantree vlan path-cost command.
Role	The role of the port for this Spanning Tree instance. Possible port roles are: root , designated , alternate , and backup .

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree cist ports	Displays Spanning Tree port information for the flat mode CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.
show spantree msti ports	Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.
show spantree vlan ports	Displays Spanning Tree port information for VLAN instances when the switch is operating in the per-VLAN 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
  vStpPortConfigPVST
  vStpPortConfigStatePVST
  vStpBridgeModePVST
```

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 10K, 6900

Usage Guidelines

- This command displays Spanning Tree port information for the flat mode CIST instance regardless of which mode (per-VLAN or flat) is active for the switch.
- Note that minimal information is displayed when this command is used in the per-VLAN mode, as the CIST is not active in this mode.

Examples

```
-> show spantree cist ports
```

```
Spanning Tree Port Summary for Cist
```

Port	Oper St	Path Cost	Desig Cost	Prim. Role	Op Port	Op Cnx	Op Edg	Desig Bridge ID	Note
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
```

Port	Oper St	Path Cost	Desig Cost	Role	Prim. Port	Op Cnx	Op Edg	Desig	Bridge ID	Note
1/1	FORW	200000	52	ROOT	1/1	PTP	EDG	8000-00:30:f1:5b:37:73		

```
-> show spantree cist ports
```

```
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
```

```
INACTIVE Spanning Tree Parameters
```

Port	Oper St	Path Cost	Desig Cost	Role	Prim. Port	Op Cnx	Op Edg	Desig	Bridge ID	Note
1/1	DIS	0	0	DIS	1/1	NS	NO	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		

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the spantree vlan 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 (nonsignificant). Shows the current operational state of the port connection type. See the spantree vlan connection command for more information.
Op Edg	Operational connection type: EDG . Shows the current operational state of the port connection type. See the spantree vlan connection command for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port 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  Cfg Stat
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
  1/1   7  ENA  No     0  AUT  No  Yes  No    No    AUT  Off
  1/2   7  ENA  No     0  NPT  No  Yes  No    No    AUT  Off
  1/3   7  ENA  No     0  NPT  No  Yes  No    No    AUT  Off
  1/4   7  ENA  No     0  NPT  No  Yes  No    No    AUT  Off
  1/5   7  ENA  No     0  NPT  No  Yes  No    No    AUT  O
```

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Port Pri	The Spanning Tree priority for the port. The lower the number, the higher the priority.
Adm St	The Spanning Tree administrative status of the port: enabled or disabled .
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 spantree vlan path-cost command.
Config Cost	The configured path cost value for this port. Configured through the spantree vlan path-cost command.
Adm Cnx	The administrative connection type: PTP , NPT , or AUT . Configured through the spantree vlan 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 spantree vlan 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 spantree cist auto-edge or spantree vlan 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 spantree cist restricted-tcn or spantree vlan 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 spantree cist restricted-role or spantree vlan restricted-role command.

Release History

Release 7.1.1; command introduced.

Related Commands

[show spantree ports](#)

Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.

[show spantree msti ports](#)

Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN 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

<i>msti_id</i>	An existing MSTI ID number.
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
<i>msti_id</i>	all MSTIs
forwarding blocking active configured	all ports

Platforms Supported

OmniSwitch 10K, 6900

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 command displays Spanning Tree port information for an MSTI regardless of which mode (per-VLAN or flat) is active on the switch.
- Note that minimal information is displayed when this command is used in the per-VLAN mode, as MSTIs are not active in this mode. In addition, if MSTP is not the selected flat mode protocol, this command fails.
- 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 0 ports
```

```
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
```

```
INACTIVE Spanning Tree Parameters
```

Port	Oper St	Path Cost	Desig Cost	Role	Prim. Port	Op Cnx	Op Edg	Desig	Bridge ID	Note
1/1	DIS	0	0	DIS	1/1	NS	NO	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		

```
-> show spantree msti 0 ports configured
```

```
Spanning Tree Port Admin Configuration for Vlan 1
```

Port	Port Pri	Adm St.	Man. Mode	Config Cost	Adm Cnx	Adm Edg	Aut Edg	Rstr Tcn	Rstr Root	Role/ Guard	PVST+ Cfg	Stat
1/1	7	ENA	No	0	AUT	No	Yes	No	No	No	AUT	Off
1/2	7	ENA	No	0	NPT	No	Yes	No	No	No	AUT	Off
1/3	7	ENA	No	0	NPT	No	Yes	No	No	No	AUT	Off
1/4	7	ENA	No	0	NPT	No	Yes	No	No	No	AUT	Off
1/5	7	ENA	No	0	NPT	No	Yes	No	No	No	AUT	Off

output definitions

Msti	The Multiple Spanning Tree Instance (MSTI) number. MSTI 0 represents the CIST. Configured through the spantree msti command.
Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Oper St	The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
Path Cost	The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the spantree msti 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.
RSTR Role/ Root Guard	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 (nonsignificant). Shows the current operational state of the port connection type. See the spantree vlan connection command for more information.

output definitions (continued)

Op Edg	Operational connection type: EDG . Shows the current operational state of the port connection type. See the spantree vlan connection command for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port segment.
PVST+ Cfg	Indicates the current PVST+ port configuration (auto, enable or disable).
PVST+ Stat	Indicates the current status of the PVST+ mode (On or Off).

```
-> show spantree msti 2 ports configured
```

```
Spanning Tree Port Admin Configuration for Msti 2
```

Port	Pri	St.	Man.	Config	Adm Cnx	Adm Edg	Aut Edg	Rstr Tcn	Rstr Root	Role/Guard	Opt.
1/1	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/2	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/3	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/4	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/5	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/6	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/7	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/8	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/9	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/10	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/11	7	ENA	No	0	AUT	No	Yes	No	No		DIS
1/12	7	ENA	No	0	AUT	No	Yes	No	No		DIS

output definitions

Port	The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
Port Pri	The Spanning Tree priority for the port. It is a numeric value and the lower the number, the higher the priority. Configured through the spantree priority command.
Adm St	The Spanning Tree administrative status of the port: enabled - ENA or disabled - DIS.
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 spantree vlan path-cost command.
Config Cost	The configured path cost value for this port. Configured through the spantree msti path-cost command.
Adm Cnx	The administrative connection type: PTP , NPT , or AUT . Configured through the spantree vlan 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 spantree vlan 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 spantree cist auto-edge or spantree vlan 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 spantree cist restricted-tcn or spantree vlan 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 spantree cist restricted-role or spantree vlan restricted-role command.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree ports	Displays Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.
show spantree cist ports	Displays Spanning Tree port information for a CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.
show spantree vlan ports	Displays Spanning Tree port information for a VLAN when the switch is operating in the per-VLAN or flat Spanning Tree mode.

MIB Objects

vStpInsPortTable
 vStpInsPortNumber
 vStpInsPortPriority
 vStpInsPortState
 vStpInsPortEnable
 vStpInsPortPathCost
 vStpInsPortDesignatedCost
 vStpInsPortDesignatedBridge
 vStpInsPortAdminEdge
 vStpInsPortAutoEdge
 vStpInsPortRestrictedRole
 vStpInsPortRestrictedTcn
 vStpInsPortManualMode
 vStpInsPortRole
 vStpPortConfigPVST
 vStpPortConfigStatePVST
 vStpBridgeModePVST
 vStpInsPrimaryPortNumber
 vStpInsPortAdminConnectionType
 vStpInsPortOperConnectionType

show spantree vlan ports

Displays Spanning Tree port information for a VLAN instance.

show spantree vlan [*vlan_id*[-*vlan_id2*]] **ports** [**forwarding** | **blocking** | **active** | **configured**]

Syntax Definitions

<i>vlan_id</i> [- <i>vlan_id2</i>]	An existing VLAN ID number. Use a hyphen to specify a range of VLAN IDs (10-15)
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
<i>vlan_id</i>	all VLAN instances
forwarding blocking active configured	all ports

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If a *vlan_id* 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 vlan 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 command displays Spanning Tree port information for a VLAN instance regardless of which mode (per-VLAN or flat) is active for 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 a VLAN ID is specified with this command. In addition, this keyword cannot be used in combination with either the **forwarding** or **blocking** keywords.

Examples

```
-> show spantree vlan ports
```

Vlan	Port	Oper	Status	Path	Cost	Role	Note
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 vlan 1 ports
```

```
Spanning Tree Port Summary for Vlan 1
```

Port	Oper St	Path Cost	Desig Cost	Role	Prim. Port	Op Cnx	Op Edg	Desig	Bridge ID	Note
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 vlan 1 ports active
```

```
Spanning Tree Port Summary for Vlan 1
```

Port	Oper St	Path Cost	Desig Cost	Role	Prim. Port	Op Cnx	Op Edg	Desig	Bridge ID	Note
1/12	FORW	19	0	DIS	1/12	PTP	EDG	0001-00:d0:95:6a:79:50		

```
-> show spantree vlan 10-13 ports
```

```
Spanning Tree Port Summary for Vlan 10
```

Port	Oper St	Path Cost	Desig Cost	Role	Prim. Port	Op Cnx	Op Edg	Desig	Bridge ID	Note
1/46	DIS	0	0	DIS	1/46	NS	EDG	0000-00:00:00:00:00:00		

```
Spanning Tree Port Summary for Vlan 11
```

Port	Oper St	Path Cost	Desig Cost	Role	Prim. Port	Op Cnx	Op Edg	Desig	Bridge ID	Note
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      Note
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  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      Note
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  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 spantree vlan 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 (nonsignificant). Shows the current operational state of the port's connection type. See the spantree vlan connection command for more information.
Op Edg	Operational connection type: EDG . Shows the current operational state of the port's connection type. See the spantree vlan connection command for more information.
Desig Bridge ID	The bridge identifier for the designated bridge for this port's segment.


```
-> show spantree vlan 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  Cfg  Stat
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
1/1   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/2   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/3   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/4   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/5   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/6   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/7   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/8   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/9   7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/10  7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/11  7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/12  7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
```

```
-> show spantree vlan 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  Cfg  Stat
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
1/46  7   ENA  No       0  AUT  No  Yes  No   No   No   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  Cfg  Stat
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
1/36  7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/37  7   ENA  No       0  AUT  No  Yes  No   No   No   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  Cfg  Stat
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
1/42  7   ENA  No       0  AUT  No  Yes  No   No   No   AUT OFF
1/43  7   ENA  No       0  AUT  No  Yes  No   No   No   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  Cfg  Stat
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
1/38  7   ENA  No       0  AUT  No  Yes  No   No   No   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 spantree priority command.
Adm St	The Spanning Tree administrative status of the port: enabled or disabled . Configured through the spantree vlan 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 spantree vlan mode command.
Config Cost	The configured path cost value for this port. Configured through the spantree vlan path-cost command.
Adm Cnx	The administrative connection type: PTP , NPT , or AUT . Configured through the spantree vlan path-cost 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 spantree vlan 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 spantree cist auto-edge or spantree vlan 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 spantree cist restricted-tcn or spantree vlan 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 spantree cist restricted-role or spantree vlan restricted-role command.
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 spantree pvst+compatibility command.
PVST+ Stat	Indicates whether or not the PVST+ interoperability status is enabled (ENA) or disabled (DIS) for the port. Configured through the spantree pvst+compatibility command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show spantree ports	Displays Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.
show spantree cist ports	Displays Spanning Tree port information for a CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.
show spantree msti ports	Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN 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 mode

Displays the current global Spanning Tree mode parameter values for the switch.

show spantree mode

Syntax Definition

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

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

spantree mode	Assigns a flat Spanning Tree or per-VLAN Spanning Tree operating mode for the switch.
spantree 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.
spantree 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.
spantree pvst+compatibility	Enables or disables PVST+ mode on the switch, port or link aggregate enabling them to operate with Cisco switches.
spantree auto-vlan-containment	Enables or disables Auto VLAN Containment (AVC).

Release History

Release 7.1.1; command introduced.

MIB Objects

```
vStpTable
  vStpMode
vStpInsTable
  vStpInsProtocolSpecification
vStpBridge
  vStpPathCostMode
vStpMstRegionTable
  vStpBridgeModePVST
vStpBridge
  vStpBridgeAutoVlanContainment
```

show spantree mst

Displays the Multiple Spanning Tree (MST) information for a MST region or the specified port or link aggregate on the switch.

show spantree mst {**region** | **port** *slot/port* / **linkagg** *linkagg_id*}

Syntax Definitions

slot/port Specifies the slot number for the module and the physical port number on that module.

linkagg_id Link aggregate ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 per-VLAN or flat Spanning Tree mode.
- Specify the port number or link aggregate ID along with the **port** or **linkagg** keyword to get information related to the specified port or link aggregate.

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
```

```
-> show spantree mst port 1/2
```

```
MST  Role  State Pth Cst  Edge Boundary Op Cnx Vlans
---+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  0   DIS   DIS     0   NO    YES      NS    1
 12   DIS   DIS     0   NO    YES      NS
```

```
-> show spantree mst linkagg 4
```

```
MST  Role  State Pth Cst  Edge Boundary Op Cnx Vlans
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
  0  DESG   FORW      6000  NO    NO      NS    1
  1  DESG   FORW      0      NO    NO      NS
  2  DESG   FORW      0      NO    NO      NS
```

output definitions

Configuration Name	An alphanumeric string that identifies the name of the MST region. Use the spantree mst region name command to define this value.
Revision Level	A numeric value that identifies the MST region revision level for the switch.
Configuration Digest	An MST region identifier consisting of a 16 octet hex value (as per the IEEE 802.1Q 2005 standard) that represents all defined MSTIs and their associated VLAN ranges. Use the spantree msti and spantree msti vlan commands to define VLAN to MSTI associations.
Revision Max hops	The number of maximum hops authorized for region information. Configured through the spantree 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 7.1.1; command introduced.

Related Commands

show spantree msti vlan-map	Displays the range of VLANs associated to the specified MSTI.
show spantree cist vlan-map	Displays the range of VLANs associated to the CIST instance.
show spantree map-msti	Displays the MSTI that is associated to the specified VLAN

MIB Objects

```
vStpMstRegionTable
  vStpMstRegionNumber
  vStpMstRegionConfigDigest
  vStpMstRegionConfigName
  vStpMstRegionConfigRevisionLevel
  vStpMstRegionCistInstanceNumber
  vStpMstRegionMaxHops
```

show spantree msti vlan-map

Displays the range of VLANs associated with the specified Multiple Spanning Tree Instance (MSTI).

```
show spantree msti [msti_id] vlan-map
```

Syntax Definitions

msti_id An existing MSTI ID number.

Defaults

By default, the VLAN to MSTI mapping is displayed for all MSTIs.

Platforms Supported

OmniSwitch 10K, 6900

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 per-VLAN or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance.

Examples

```
-> show spantree msti vlan-map
```

```
Cist
Name          :
VLAN list     : 1-9,14-4094
```

```
Msti 1
Name          :
VLAN list     : 10-11
```

```
Msti 2
Name          :
VLAN list     : 12-13
```

```
-> show spantree msti 2 vlan-map
```

```
Msti 2
Name          : MS1,
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.

output definitions (continued)

Name	An alphanumeric value that identifies an MSTI name. Use the spantree msti command to define an MSTI name.
VLAN list	The range of VLAN IDs that are associated with this MSTI.

Release History

Release 7.1.1; command introduced.

Related Commands

show spantree mst	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 10K, 6900

Usage Guidelines

This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.

Examples

```
-> show spantree cist vlan-map
```

```
Cist
Name           : CIST1,
VLAN list      : 1-9,14-4094
```

output definitions

Name	An alphanumeric value that identifies the name of the CIST. Use the spantree 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 7.1.1; command introduced.

Related Commands

show spantree mst	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 [vlan vlan_id] map-msti
```

Syntax Definitions

vlan_id An existing VLAN ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance.

Examples

```
-> show spantree map-msti
```

```
Vlan   Msti/Cist(0)
-----+-----
   200      1
```

Release History

Release 7.1.1; command introduced.

Related Commands

- show spantree mst** 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
```

7 Shortest Path Bridging Commands

The Alcatel-Lucent OmniSwitch supports Shortest Path Bridging MAC (SPBM), as defined in the IEEE 802.1aq standard. SPB-M uses the Provider Backbone Bridge (PBB) network model to encapsulate (using IEEE 802.1ah headers) and tunnel customer traffic through the network backbone. The shortest path trees (SPTs) upon which the PBB network infrastructure operates are determined using a version of the Intermediate System-to-Intermediate System (IS-IS) link state protocol that supports TLV extensions for SPB (ISIS-SPB).

The SPBM network topology consists of two layers: the backbone infrastructure (control plane) layer and the services (data plane) layer. ISIS-SPB builds the backbone layer by defining loop-free, SPTs through the backbone network. The service layer is based on the PBB framework as defined in the IEEE 802.1ah standard. SPBM supports the 802.1ah MAC-in-MAC method for data encapsulation. SPBM services transport the encapsulated traffic over the ISIS-SPB infrastructure.

This chapter documents the Command Line Interface (CLI) commands used to configure and verify the ISIS-SPB backbone. For commands used to configure and verify the SPBM services layer, see [Chapter 44, “Service Manager Commands.”](#)

MIB information for the SPB commands is as follows:

Filename: ALCATEL-IND1-ISIS-SPB-MIB
Module: alcatelIND1IsisSpbMib

Filename: ALCATEL-IND1-VLAN-MGR-MIB
Module: alcatelIND1VLANMgrMIB

A summary of the available commands is listed here:

Global ISIS-SPB Commands	spb isis admin-state spb isis area-address spb isis bridge-priority spb isis source-id spb isis spf-wait spb isis lsp-wait
Backbone VLAN (BVLAN) Commands	spb bvlan spb isis bvlan ect-id spb isis control-bvlan spb isis bvlan tandem-multicast-mode
Interface Commands	spb isis interface

Graceful Restart Commands	spb isis graceful-restart spb isis graceful-restart helper
Show Commands	show spb isis info show spb isis bvlans show spb isis interface show spb isis adjacency show spb isis database show spb isis nodes show spb isis unicast-table show spb isis services show spb isis spf show spb isis multicast-table show spb isis multicast-sources show spb isis multicast-sources-spf show spb isis ingress-mac-filter

spb bvlan

Configures an SPB backbone VLAN (BVLAN).

spb bvlan {*bvlan_id*[-*bvlan_id2*]} [**admin-state** {**enable** | **disable**}] [**name** *description*] [**tunnel-mtu** *mtu*]

no spb bvlan *bvlan_id*

Syntax Definitions

<i>bvlan_id</i> [- <i>bvlan_id2</i>]	A numeric value that uniquely identifies an individual BVLAN. The valid ID range is 1–4094. Use a hyphen to specify a range of BVLAN IDs (10-20).
enable	Enables the VLAN administrative status.
disable	Disables the VLAN administrative status.
<i>description</i>	An alphanumeric string. Optional name description for the VLAN ID.
<i>mtu</i>	The tunnel maximum transmission unit (MTU) packet size allowed for all ports associated with the BVLAN. The valid range is 1280–9198.

Defaults

parameter	default
enable disable	enable
<i>description</i>	VLAN ID
<i>mtu</i>	1524

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a BVLAN from the switch configuration. All BVLAN ports are detached before the BVLAN is removed.
- The description can be any alphanumeric string. Enclose the description in double quotes if it contains more than one word with a space in between.
- The BVLAN configuration must be the same on each SPB bridge to ensure proper ISIS-SPB neighbor discovery and shortest path calculations throughout the provider backbone bridge (PBB) network.
- BVLANs differ from standard VLANs as follows:
 - No Spanning Tree control—the Spanning Tree protocol is automatically disabled on each BVLAN, and all ports associated with each BVLAN will remain in a forwarding state. However, Spanning Tree can remain operational on other types of VLANs.
 - No source MAC address learning—normal hardware learning is disabled on BVLANs. Instead, the forwarding database (FDB) is populated by the ISIS-SPB protocol.
 - There is no flooding of unknown destination or multicast frames.

- Ingress filtering based on the source MAC address—frames received on ports that do not have an incoming source MAC address pre-programmed by ISIS-SPB are discarded.
- IP interfaces are not supported on BVLANS, so the MTU size is not applicable for this release.
- All BVLANS are automatically associated with all ISIS-SPB interfaces. Adding or removing BVLANS from a specific SPB interface is not allowed.
- The maximum number of BVLANS supported is four.
- BVLANS and standard VLANs can co-exist on the same bridge ports.

Examples

```
-> spb bvlan 200 name BVLAN-200
-> spb bvlan 720 admin-state disable
-> spb bvlan 500 name BVLAN-500 admin-state enable
-> no spb bvlan 1020
```

Release History

Release 7.3.1; command introduced.

Related Commands

spb isis control-bvlan	Configures a control BVLAN
spb isis bvlan ect-id	Assigns an equal cost tree (ECT) algorithm ID to the specified BVLAN.
spb isis bvlan tandem-multicast-mode	Configures the tandem multicast mode for the specified SPB backbone VLAN (BVLAN).
spb isis interface	Configures ISIS-SPB network interfaces.
show spb isis bvlan	Displays the BVLAN configuration for the switch.

MIB Objects

```
vlanTable
  vlanNumber
  vlanDescription
  vlanAdmStatus
  vlanOperStatus
  vlanType
  vlanMtu
```

spb isis bvlan ect-id

Configures the equal cost tree (ECT) identifier for the specified SPB backbone VLAN (BVLAN). The ECT ID assigns a tie-breaking algorithm to the BVLAN that is used for shortest path tree (SPT) calculations.

```
spb isis bvlan bvlan_id ect-id ect_id
```

Syntax Definitions

<i>bvlan_id</i>	An existing BVLAN ID.
<i>ect_id</i>	An ECT algorithm ID. The valid range is 1–16.

Defaults

By default, the next available ECT ID number is automatically assigned to a BVLAN when the BVLAN is created.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to change the existing ECT ID number for the specified BVLAN on each SPB bridge, as necessary, to make sure the specified BVLAN uses the same ECT ID throughout the network.
- The BVLAN ID specified with this command must already exist in the switch configuration.

Examples

```
-> spb isis bvlan 200 ect-id 5  
-> spb isis bvlan 720 ect-id 10
```

Release History

Release 7.3.1; command introduced.

Related Commands

spb bvlan	Creates a SPB backbone VLAN (BVLAN).
show spb isis bvlan	Displays the SPB BVLAN configuration for the switch.

MIB Objects

```
alcatelIND1IsisSpbEctStaticTable  
  alcatelIND1IsisSpbEctStaticEntryBaseVid
```

spb isis control-bvlan

Designates an existing BVLAN that will serve as the control BVLAN for the bridge. Only one BVLAN per bridge is designated as the control BVLAN, which is used to exchange ISIS-SPB control packets with neighboring SPB bridges on behalf of all the BVLANs configured for that bridge.

spb isis control-bvlan *bvlan_id*

Syntax Definitions

bvlan_id An existing BVLAN ID.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The BVLAN ID specified with this command must already exist in the switch configuration.
- The control BVLAN ID is the VLAN tag that is applied to ISIS-SPB control frames.
- Configuring an existing BVLAN as the control BVLAN does not exclude that VLAN from carrying data traffic for the SPB domain. In other words, a single VLAN can serve as both a regular BVLAN and the control BVLAN at the same time.

Examples

```
-> spb isis control-bvlan 200
-> spb isis control-bvlan 720
```

Release History

Release 7.3.1; command introduced.

Related Commands

[spb bvlan](#) Configures an SPB BVLAN.
[show spb isis bvlan](#) Displays the BVLAN configuration for the bridge.

MIB Objects

```
alcatelIND1IsisSpbSys
  alcatelIND1IsisSpbSysControlBvlan
```

spb isis bvlan tandem-multicast-mode

Configures the tandem multicast mode for the specified SPB backbone VLAN (BVLAN). This mode is only applicable to associated SPB service instances that are configured to use the tandem replication mode for multicast traffic.

```
spb isis bvlan bvlan_id tandem-multicast-mode {sgmode | gmode}
```

Syntax Definitions

<i>bvlan_id</i>	An existing BVLAN ID.
sgmode	Specifies the source and group (S,G) mode for the BVLAN.
gmode	Specifies the any source and group (*,G)

Defaults

By default, BVLANS are configured to use the (S,G) mode.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The BVLAN ID specified with this command must already exist in the switch configuration.
- The (S,G) mode identifies a source-specific multicast distribution tree.
- The (*,G) mode identifies a shared multicast distribution tree.

Examples

```
-> spb isis bvlan 200 tandem-multicast-mode gmode  
-> spb isis bvlan 720 tandem-multicast-mode sgmode
```

Release History

Release 7.3.1; command introduced.

Related Commands

spb bvlan	Creates a SPB backbone VLAN (BVLAN).
show spb isis bvlan	Displays the SPB BVLAN configuration for the switch.

MIB Objects

```
alcatelIND1IisisSpbEctStaticTable  
  alcatelIND1IisisSpbEctStaticEntryBaseVid  
  alcatelIND1IisisSpbEctStaticEntryMulticastMode
```

spb isis bridge-priority

Configures the bridge priority value for the SPB bridge. This value is used to rank an SPB bridge in relation to other bridges.

spb isis bridge-priority *priority*

Syntax Definitions

priority A bridge priority value. The valid range is 0–65535.

Defaults

By default, the bridge priority value for the switch is set to 32768.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The lower the bridge priority number assigned, the higher the priority that is associated with the bridge.
- The bridge priority value makes up the upper two bytes of the eight-byte SPB bridge ID. The lower six bytes of the Bridge ID contain the system ID, which is the dedicated bridge MAC address of the SPB bridge.
- Setting a different bridge priority value on different SPB bridges will override the system identifier significance during the shortest path tree (SPT) calculation.

Examples

```
-> spb isis bridge-priority 15  
-> spb isis bridge-priority 32768
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show spb isis info](#) Displays the status and configuration information for the SPB bridge.

MIB Objects

```
alcatelIND1IisisSpbSys  
alcatelIND1IisisSpbSysBridgePriority
```

spb isis interface

Configures the specified port or link aggregate as an ISIS-SPB interface on which protocol data units (PDUs) are sent and received to detect neighbors and form adjacencies with other SPB bridges in the network.

spb isis interface {port *slot/port*[-*port2*] / linkagg *agg_id*[-*agg_id2*]} [admin-state {enable | disable}] [hello-interval *seconds*] [hello-multiplier *count*] [metric *metric*]

no spb isis interface [port *chassis/slot/port*[-*port2*] / linkagg *agg_id*[-*agg_id2*]]

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i> [- <i>agg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Administratively enables the SPB interface.
disable	Administratively disables the SPB interface.
<i>seconds</i>	The amount of time, in seconds, to wait between each transmission of a hello packet from this interface. The valid range is 1–20000.
<i>count</i>	An integer value that is multiplied by the hello interval time to determine the amount of time, in seconds, a receiving bridge holds onto the hello packets transmitted from this interface. The valid range is 2–100.
<i>metric</i>	An integer value that specifies the link cost to reach the destination BMAC. The valid range is 1–16777215.

Defaults

parameter	default
enable disable	enable
<i>seconds</i>	9
<i>count</i>	3
<i>metric</i>	10

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the ISIS-SPB interface.
- When configuring a link aggregate as an SPB interface, make sure the link aggregate ID number already exists in the switch configuration.

- All SPB interfaces are automatically assigned to all existing BVLANs. There is one ISIS-SPB instance per switch, and each BVLAN and SPB interface are associated with that instance.
- If the SPB interface metric value is set to a different value for each side of a link, the highest metric value is applied to the entire link.
- Administratively enabling ISIS-SPB on the switch triggers ISIS hello packet transmissions on all SPB interfaces.
- SPB interfaces are typically the Network Network Interface (NNI) ports that carry encapsulated customer data traffic through the Provider Backbone Bridging (PBB) network.
- Note that configuring a port or link aggregate as an SPB interface does not prevent configuration of other VLAN tagging on that port. In other words, the SPB interface can forward regular traffic for other VLAN types in addition to encapsulated SPBM traffic.

Examples

```
-> spb isis interface port 4/7
-> spb isis interface port 4/7 hello-interval 60
-> spb isis interface linkagg 3
-> spb isis interface linkagg 3 hello-multiplier 10
-> spb isis interface port 1/10 hello-interval 20 hello-multiplier 5 metric 2
-> no spb isis interface port 4/7
-> no spb isis interface linkagg 3
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show spb isis interface](#) Displays the ISIS-SPB interface configuration for the bridge.

MIB Objects

```
alcatelIND1IisisSpbAdjStaticTable
  alcatelIND1IisisSpbAdjStaticEntryIfIndex
  alcatelIND1IisisSpbAdjStaticEntryMetric
  alcatelIND1IisisSpbAdjStaticEntryHelloInterval
  alcatelIND1IisisSpbAdjStaticEntryHelloMultiplier
  alcatelIND1IisisSpbAdjStaticEntryIfAdminState
```

spb isis admin-state

Enables or disables the administrative status of ISIS-SPB instance for the switch.

spb isis admin-state {enable | disable}

Syntax Definitions

enable Administratively enables ISIS-SPB for the switch.
disable Administratively disables ISIS-SPB for the switch.

Defaults

parameter	default
enable / disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When the ISIS-SPB status is disabled, the configuration settings and related statistics of the protocol remain unaffected.

Examples

```
-> spb isis admin-state enable  
-> spb isis admin-state disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show spb isis info](#) Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IisisSpbSys  
  alcatelIND1IisisSpbSysAdminState
```

spb isis area-address

Configures the area address for the ISIS-SPB instance.

```
spb isis area-address area_address
```

Syntax Definitions

area_address A 3-byte integer that specifies the ISIS-SPB area address to join.

Defaults

By default, the area address is set to 0.0.0. for ISIS-SPB.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The default setting of 0.0.0 is the area address typically used for ISIS-SPB.
- Changing the area address with this command is allowed, but make sure to configure each bridge that will participate in the ISIS-SPB instance with the same area address value.
- ISIS-SPB and ISIS-IP instances may co-exist on the same bridge.

Examples

```
-> spb isis area-address 1.1.1  
-> spb isis area-address 0.0.0
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show spb isis info](#) Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IsisSpbSys  
  alcatelIND1IsisSpbSysAreaAddress
```

spb isis source-id

Configures the shortest path (SP) source identifier value for the SPB bridge. This value identifies the source of multicast frames and is relevant only in multicast tandem replication mode.

```
spb isis source-id {source_id | auto}
```

Syntax Definitions

<i>source_id</i>	A source identifier entered as <i>xx-xx-xx</i> , where <i>xx</i> is a hexadecimal value.
auto	Changes the source ID back to the default value.

Defaults

By default, the last three least significant bytes of the system ID is used for the source ID.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The source ID is the high order 3 bytes for the Group Address DA for the SPB bridge. Note that only 20 bits are used; the top 4 bits are not used.

Examples

```
-> spb isis source-id 00-2a-1d
-> spb isis source-id 07-0b-d3
-> spb isis source-id auto
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show spb isis info](#) Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IisisSpbSys
  alcatelIND1IisisSpbmSysSPSourceId
```

spb isis spf-wait

Configures the time intervals between the first, second, and subsequent ISIS-SPB shortest path first (SPF) calculations.

spb isis spf-wait [**initial-wait** *milliseconds* | **second-wait** *milliseconds*] **max-wait** *milliseconds*]

Syntax Definitions

max-wait <i>milliseconds</i>	Specifies the maximum number of milliseconds to wait between two consecutive SPF calculations. Enter a value that is the same or greater than the second wait time value. The valid range is 1000–120000 milliseconds.
initial-wait <i>milliseconds</i>	Specifies the number of milliseconds to wait before triggering an initial SPF calculation after a topology change. The valid range is 10–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.
second-wait <i>milliseconds</i>	Specifies the minimum number of milliseconds to wait between the first and second SPF calculation. The valid range is 1–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.

Defaults

parameter	default
max-wait <i>milliseconds</i>	1000
initial-wait <i>milliseconds</i>	100
second-wait <i>milliseconds</i>	300

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- To reset all three of the SPF wait time intervals back to their default values, use the **spb isis spf-wait** command without specifying any parameters.
- Subsequent SPF calculations, if required, are generated at exponentially increasing intervals of the SPF **second-wait** parameter value until the **maximum-wait** parameter value is reached. For example, if the second-wait interval value is set to 1000 milliseconds, then the next SPF calculation is triggered after 2000 milliseconds and the next SPF calculation after that is triggered at 4000 milliseconds, and so on, until the maximum-wait interval value is reached.
- When the maximum interval value is reached, the SPF wait interval will stay at the maximum value until there are no more SPF calculations scheduled during that interval. After a full interval without any SPF calculations, the SPF wait interval will reset back to the **initial-wait** parameter interval value.

Examples

```
-> spb isis spf-wait max-wait 2500 initial-wait 1000 second-wait 1500
-> spb isis spf-wait max-wait 5000
-> spb isis spf-wait initial-wait 1000
-> spb isis spf-wait second-wait 2000
-> spb isis spf-wait
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[spb isis lsp-wait](#)

Configures the time intervals between the first, second, and subsequent generation of link state PDUs (LSPs).

[show spb isis info](#)

Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IisisSpbProtocolConfig
  alcatelIND1IisisSpbProtocolSpfMaxWait
  alcatelIND1IisisSpbProtocolSpfInitialWait
  alcatelIND1IisisSpbProtocolSpfSecondWait
```

spb isis lsp-wait

Configures the time intervals between the first, second and subsequently generated link state PDU (LSP).

```
spb isis lsp-wait {max-wait milliseconds | initial-wait milliseconds| second-wait milliseconds}
```

Syntax Definitions

max-wait <i>milliseconds</i>	Specifies the maximum number of seconds to wait between two consecutively generated LSPs. Enter a value that is the same or greater than the second wait time value. The valid range is 1000–120000 milliseconds.
initial-wait <i>milliseconds</i>	Specifies the number of seconds to wait before triggering an initial LSP generation after a topology change. The valid range is 0–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.
second-wait <i>milliseconds</i>	Specifies the minimum number of seconds to wait between the first and second generated LSPs. The valid range is 1000–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.

Defaults

parameter	default
max-wait <i>milliseconds</i>	1000
initial-wait <i>milliseconds</i>	0
second-wait <i>milliseconds</i>	300

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- To reset all three of the LSP wait time intervals back to their default values, use the **spb isis lsp-wait** command without specifying any parameters.
- Subsequent LSP, if required, are generated at exponentially increasing intervals of the LSP **second-wait** parameter value until the **maximum-wait** parameter value is reached. For example, if the second-wait interval value is set to 10 seconds, then the next LSP is generation is triggered after 20 seconds and the next LSP generated after that is triggered at 40 seconds, and so on, until the maximum-wait interval value is reached.
- When the maximum interval value is reached, the LSP wait interval will stay at the maximum value until there are no more LSP generations during that interval. After a full interval without any LSP generations, the LSP wait interval will reset back to the **initial-wait** parameter interval value.

Examples

```
-> spb isis lsp-wait max-wait 2000 initial-wait 1000 second-wait 1500
-> spb isis lsp-wait max-wait 5000
```

```
-> spb isis lsp-wait initial-wait 2500
-> spb isis lsp-wait second-wait 3000
-> spb isis lsp-wait
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis spf-wait	Configures the time intervals between the first, second, and subsequent shortest path first (SPF) calculations.
show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IisisSpbProtocolConfig
  alcatelIND1IisisSpbProtocolLspMaxWait
  alcatelIND1IisisSpbProtocolLspInitialWait
  alcatelIND1IisisSpbProtocolLspSecondWait
```

spb isis overload

Configures the LSP database overload state for the local ISIS-SPB switch and optionally specifies the amount of time the switch remains in this state. When the overload state is enabled, the switch signals to other ISIS-SPB switches that it is not able to accept transit traffic.

spb isis overload [**timeout** *seconds*]

no spb isis overload

Syntax Definitions

seconds Specifies the timeout interval, in seconds. The valid range is 60–1800.

Defaults

By default, the IS-IS overload state is disabled.

parameter	default
<i>seconds</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to make the router exit the overload state.
- If the time period is not specified, the router remains in the overload state for an infinite period.
- During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is used only if the destination route is directly reachable by the router (for example, it will not be used for other transit traffic).
- This command can be used when the router is overloaded or before executing a shutdown command to divert traffic around the router.

Examples

```
-> spb isis overload timeout 70  
-> no spb isis overload
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[spb isis overload-on-boot](#)

Configures the ISIS-SPB instance to operate in an overload state during bootup for a specified time period.

[show spb isis info](#)

Displays status and configuration information for the ISIS-SPB instance.

MIB Objects

```
alcatelIND1IisisSpbSysSetOverload  
alcatelIND1IisisSpbSysOverloadTimeout  
alcatelIND1IisisSpbSysOverloadStatus
```

spb isis overload-on-boot

Configures the ISIS-SPB switch to operate in the overload state after a system bootup for the specified amount of time.

spb isis overload-on-boot [*timeout seconds*]

no spb isis overload-on-boot

Syntax Definitions

seconds Specifies the timeout interval, in seconds. The valid range is 60–1800.

Defaults

By default, the ISIS-SPB switch will not operate in the overload state after a bootup.

parameter	default
<i>seconds</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to prevent the switch from entering the overload state after bootup.
- An ISIS-SPB switch operating in the overload state is used only if there is no alternate path to reach the destination.
- This command configures the switch to operate in the overload state after a bootup and until the timeout value expires or the **no** form of this command is used.
- The **no spb isis overload** command does not influence the overload-on-boot function.

Examples

```
-> spb isis overload-on-boot timeout 80  
-> no spb isis overload-on-boot
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis overload

Sets the ISIS-SPB switch to operate in the overload state.

show spb isis info

Displays status and configuration information for the ISIS- SPB instance.

MIB Objects

vRtrIisisTable

alcatelIND1IisisSpbSysOverloadOnBoot

alcatelIND1IisisSpbSysOverloadOnBootTestTimeout

alcatelIND1IisisSpbSysOverloadStatus

spb isis graceful-restart

Configures graceful restart of the bridge. It allows ISIS-SPB to reconverge faster, minimizing service interruption.

spb isis graceful-restart

no spb isis graceful-restart

Syntax Definitions

N/A

Defaults

By default, the graceful restart functionality is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable graceful restart and remove the graceful restart configuration from the SPB bridge.
- When graceful restart is enabled, the bridge can either be a helper (which helps a neighbor router to restart) or a restarting router, or both.

Examples

```
-> spb isis graceful-restart  
-> no spb isis graceful-restart
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[spb isis graceful-restart helper](#) Configures the helper mode of routers for graceful restart.

[show spb isis info](#) Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IisisSpbProtocolConfig  
  alcatelIND1IisisSpbProtocolGracefulRestart
```

spb isis graceful-restart helper

Administratively enables and disables the ISIS-SPB bridge to operate in the helper mode in response to a bridge performing a graceful restart.

spb isis graceful-restart helper {enable | disable}

Syntax Definitions

enable	Enables the helper mode on the bridge.
disable	Disables the helper mode on the bridge.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When graceful restart is enabled, the helper mode is enabled by default.

Examples

```
-> spb isis graceful-restart helper disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis graceful-restart	Configures graceful restart on the bridge.
show spb isis info	Displays status and configuration information for the SPB instance.

MIB Objects

```
alcatelIND1IisisSpbProtocolConfig  
alcatelIND1IisisSpbProtocolGRHelperMode
```

show spb isis info

Displays the global ISIS-SPB status and configuration information for the SPB bridge.

show spb isis info

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show spb isis info
SPB ISIS Bridge Info:
  System Id           = e8e7.3233.1831,
  System Hostname     = BEB-1,
  SPSourceID          = 03-18-31,
  SPBM System Mode    = auto,
  BridgePriority       = 32768 (0x8000),
  MT ID               = 0,
  Control BVLAN       = 4001,
  Area Address         = 0.0.0,
  Level Capability     = L1,
  Admin State         = UP,
  LSDB Overload       = Disabled,
  Last Enabled        = Thu Aug  2 22:43:19 2012,
  Last SPF             = Fri Aug  3 18:15:51 2012,
  SPF Wait            = Max: 1000 ms, Initial: 100 ms, Second: 300 ms,
  LSP Lifetime        = 1200,
  LSP Wait            = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
  Graceful Restart    = Disabled,
  GR helper-mode      = Disabled,
  # of L1 LSPs        = 8
```

output definitions

System Id	The system ID of the SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
System Hostname	The system name assigned to the SPB bridge. Configured through the system name command.

output definitions (continued)

SPSourceID	The shortest path (SP) source ID value for the SPB bridge. This value identifies the source of multicast frames and is relevant only in the multicast tandem replication mode. Configured through the spb isis source-id command.
SPBM System Mode	Indicates if the SP source ID was manually set (manual) using the spb isis source-id command or automatically allocated (auto) using the last three least significant bytes of the System ID.
BridgePriority	The bridge priority value assigned to the SPB bridge. Configured through the spb isis bridge-priority command.
MT ID	The IS-IS Multi Topology ID.
Control BVLAN	The SPB base VLAN assigned to exchange ISIS-SPB control traffic with other SPB bridges. Configured through the spb isis control-bvlan command.
Area Address	The IS-IS area address for this ISIS-SPB instance. Configured through the spb isis area-address command.
Level Capability	The level capability of the bridge. Only Level 1 (L1) is supported.
Admin State	The state of the SPB instance for the bridge (Up or Down). Configured through the spb isis admin-state command.
LSDB Overload	The LSP database overload state of the switch. Configured through the spb isis overload command.
Last Enabled	The date and time when the ISIS-SPB instance was last enabled for the bridge.
Last SPF	The date and duration of the last shortest path first (SPF) calculation.
SPF Wait	The SPF wait time intervals used to trigger SPF calculations after a topology change. Configured through the spb isis spf-wait command.
LSP Lifetime	The Lifetime of the LSP, in seconds.
LSP Wait	The LSP wait time intervals used to trigger LSP generations. Configured through the spb isis lsp-wait command.
Graceful Restart	Indicates if graceful restart is Enabled or Disabled . Configured through the spb isis graceful-restart command.
GR helper-mode	Indicates if the graceful restart helper mode is Enabled or Disabled . Configured through the spb isis graceful-restart helper command.
# of L1 LSPs	The number of LSPs for Level-1 adjacency.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis spf	Displays the shortest path first (SPF) information to all known SPB bridges for a specific BVLAN.
show spb isis vlans	Displays the ISIS-SPB backbone VLAN (BVLAN) configuration for the bridge.
show spb isis interface	Displays the ISIS-SPB network interface configuration for the bridge.

MIB Objects

```
alcatelIND1IisisSpbSys
  alcatelIND1IisisSpbSysId
  alcatelIND1IisisSpbSysName
  alcatelIND1IisisSpbmSysSPSourceId
  alcatelIND1IisisSpbmSysMode
  alcatelIND1IisisSpbSysBridgePriority
  alcatelIND1IisisSpbSysControlBvlan
  alcatelIND1IisisSpbSysAreaAddress
  alcatelIND1IisisSpbSysAdminState
  alcatelIND1IisisSpbProtocolSpfMaxWait
  alcatelIND1IisisSpbProtocolSpfInitialWait
  alcatelIND1IisisSpbProtocolSpfSecondWait
  alcatelIND1IisisSpbProtocolLspMaxWait
  alcatelIND1IisisSpbProtocolLspInitialWait
  alcatelIND1IisisSpbProtocolLspSecondWait
  alcatelIND1IisisSpbProtocolGracefulRestart
  alcatelIND1IisisSpbProtocolGRHelperMode
```

show spb isis bvlans

Displays the ISIS-SPB backbone VLAN (BVLAN) configuration for the bridge.

show spb isis nodes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command also displays the equal cost tree (ECT) algorithm that is assigned to each BVLAN.

Examples

```
-> show spb isis bvlans
SPB ISIS BVLANS:
```

BVLAN	ECT-algorithm	In Use	Services mapped	Num ISIDS	Tandem Multicast	Root Bridge (Name : MAC Address)
501	00-80-c2-01	NO	NO	0	GMODE	BRIDGE-3:00:d1:95:00:30:02
502	00-80-c2-02	NO	NO	0	SGMODE	
503	00-80-c2-03	YES	NO	4	SGMODE	
504	00-80-c2-04	YES	NO	4	SGMODE	

```
BVLANS:          4
```

output definitions

BVLAN	The VLAN ID number for the SPB BVLAN. Configured through the spb bvlan command.
ECT-algorithm	The equal cost tree (ECT) algorithm index (1–16) assigned to the BVLAN. Configured through the spb isis bvlan ect-id command.
In Use	Indicates whether or not the BVLAN is in use.
Services Mapped	Indicates whether or not any local services are mapped to the BVLAN.
Num ISIDS	The number of services known to the BVLAN.
Tandem Multicast	The tandem multicast mode (SGMODE or GMODE) for the BVLAN. Configured through the spb isis bvlan tandem-multicast-mode command.
Root Bridge (Name : MAC Address)	The system name and bridge MAC address of the root bridge. This value is displayed only for GMODE configurations.

Release History

Release 7.3.1; command was introduced.

Related Commands

[show spb isis info](#)

Displays status and configuration information for the SPB instance

[show spb isis interface](#)

Displays the ISIS-SPB network interface configuration for the bridge.

MIB Objects

N/A

show spb isis interface

Displays the ISIS-SPB network interface configuration for the switch.

show spb isis interface

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command also shows the operational and administrative status of the interface.
- When an SPB interface is created, the interface is automatically assigned to each SPB BVLAN in the switch configuration.

Examples

```
-> show spb isis interface
SPB ISIS Interfaces:
```

Interface	Level	CircID	Oper state	Admin state	Link Metric	Hello Intvl	Hello Mult
1/1	L1	1	DOWN	UP	10	9	3
1/2	L1	2	UP	UP	10	9	3
1/3	L1	3	DOWN	UP	10	9	3
1/4	L1	4	DOWN	UP	10	9	3
1/5	L1	5	DOWN	UP	10	9	3
1/6	L1	6	DOWN	UP	10	9	3
1/7	L1	7	DOWN	UP	10	9	3
1/10	L1	9	DOWN	UP	10	9	3

Interfaces : 8

output definitions

Interface	The slot/port or link aggregate ID of the SPB interface.
Level	The IS-IS Area Level (L1) for the interface.
CircID	The circuit ID of the interface.
Oper-state	The operational state of the interface (UP or DOWN).
Admin-state	The administrative state of the interface (UP or DOWN).
Link Metric	The metric value of the router for the corresponding area level.

output definitions

Hello Interval	The number of seconds the interface waits between Hello PDU transmissions.
Hello Multiplier	The number that is multiplied by the Hello Interval to determine the hold time.

Release History

Release 7.3.1; command was introduced.

Related Commands

[spb isis interface](#) Creates an ISIS-SPB network interface.

MIB Objects

N/A

show spb isis adjacency

Displays information about the ISIS-SPB adjacencies created for the SPB bridge.

show ip isis adjacency [detail]

Syntax Definitions

detail Displays additional information about the ISIS-SPB adjacencies.

Defaults

By default, a summary list of adjacency information is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip isis adjacency
SPB ISIS Adjacency:
  System
  (Name : SystemId)                Type State Hold Interface
-----+-----+-----+-----+-----
      bridge2 : 00d0.9506.4c62      L1  UP   27      1/1
      bridge3 : 00d0.9507.9732      L1  UP   20      1/2

Adjacencies : 2
```

output definitions

Name	The system name assigned to the adjacent SPB bridge.
SystemId	The system ID of the adjacent SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
Type	The level (LI) of the adjacent bridge.
State	The state of the adjacency (UP or DOWN).
Hold	The adjacency hold time, in seconds.
Interface	The slot/port or link aggregate ID of the SPB interface on which the adjacency was formed.
Adjacencies	The total number of adjacent SPB bridges.

```

-> show ip isis adjacency detail
SPB ISIS Adjacency detail:
  SystemID: 00d0.9506.4c62 :
    B-MAC      : 00:d0:95:06:4c:62      , Hostname   : bridge2      ,
    Interface  : 1/1                    , Up Time    : Mon Sep 26 17:54:29 2011,
    State      : UP                      , Priority    : 0              ,
    Hold Time  : 18                      , Max Hold   : 27              ,
    Adj Level  : L1                      , NLPIDs     : SPB            ,
    ExtLocalCktId(YES): 2,
    Restart Support : Disabled            ,
    Restart Status  : Not currently being helped,
    Restart Supressed : Disabled

  SystemID: 00d0.9507.9732 :
    B-MAC      : 00:d0:95:07:97:32      , Hostname   : bridge3      ,
    Interface  : 1/2                    , Up Time    : Mon Sep 26 17:54:29 2011,
    State      : UP                      , Priority    : 0              ,
    Hold Time  : 21                      , Max Hold   : 27              ,
    Adj Level  : L1                      , NLPIDs     : SPB            ,
    ExtLocalCktId(YES): 2,
    Restart Support : Disabled            ,
    Restart Status  : Not currently being helped,
    Restart Supressed : Disabled

```

Adjacencies : 1

output definitions

SystemID	The system ID of the adjacent SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
B-MAC	The backbone MAC address (system ID) of the adjacent bridge. This is the address that is used as the source address for encapsulated customer traffic that is tunneled through SPB services.
Interface	The slot/port or link aggregate ID of the SPB interface on which the adjacency was formed.
State	The state of the adjacency (UP or DOWN).
Hold Time	The adjacency hold time, in seconds.
Adj Level	The adjacency level (L1) of the SPB bridge.
ExtLocalCktId(YES)	The circuit ID that the peer bridge has assigned to this adjacency.
Restart Support	Indicates if graceful restart is Enabled or Disabled .
Restart Status	Indicates whether the adjacent SPB bridge is helping the local bridge to restart (Not currently being helped or Currently being helped).
Restart Suppressed	Indicates whether or not the advertisement of LSPs is suppressed per the request of adjacent SPB bridge (Enabled or Disabled).
Hostname	The system name assigned to the adjacent SPB bridge.
Up Time	Indicates the time period in seconds, during which the SPB bridge was in the adjacency.
Priority	The bridge priority value of the adjacent SPB bridge.

output definitions

Max Hold	Indicates the maximum hold time of the adjacent SPB bridge.
NLPIDs	The Network Layer Protocol ID (NLPID) of the adjacent bridge (SPB NLPID = 0xC1).

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis database	Displays ISIS-SPB topology information maintained in the link state database (LSDB).
show spb isis nodes	Displays the discovered node-level parameter values for all of the ISIS-SPB bridges participating in the topology.

MIB Objects

N/A

show spb isis database

Displays ISIS-SPB topology information maintained in the link state database (LSDB).

show ip isis database [lsp-id *lsp_id*]

Syntax Definitions

lsp_id The LSP ID.

Defaults

By default, the entire LSDB is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *lsp-id* parameter with this command to view database information for a specific link state packet (LSP).

Examples

```
-> show spb isis database
  Legends : P    = The Partition repair bit is set
            OV  = The overload bit is set
            ATT = The Attach bit is set
            L1  = Specifies a Level 1 IS type
            L2  = Specifies a Level 2 IS type
SPB ISIS LSP Database:
LSP ID          Sequence      Checksum    Lifetime    Attributes
-----+-----+-----+-----+-----
00d1.9500.3002.00-00  0x000000a8    0x9bdc      862         L1
00e0.b188.99be.00-00  0x0000009c    0xa719      762         L1
Level-1 LSP count : 2
```

output definitions

LSP ID	The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.
Sequence	The sequence number of the LSP. The sequence number is a value used to identify old and duplicate LSPs.
Checksum	The checksum value of the LSP.
Lifetime	The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the LSDB of all the SPB bridges.
Attributes	The level capability of the bridge. This implementation of ISIS-SPB only supports Level 1 (L1).
LSP Count	The number of LSPs in the LSDB.

```

-> show spb isis database lsp-id 0000.bcb4.0001.00-00
Legends : P      = The Partition repair bit is set
          OV     = The overload bit is set
          ATT    = The Attach bit is set
          L1     = Specifies a Level 1 IS type
          L2     = Specifies a Level 2 IS type
SPB ISIS LSP Database:
-----
LSP ID       : 0000.bcb4.0001.00-00          Level       : L1
Sequence     : 0x00000068                   Checksum    : 0xf4f5   Lifetime    : 1118
Version      : 1                             Pkt Type    : 18       Pkt Ver     : 1
Attributes   : L1                           Max Area    : 3
SysID Len    : 6                             Used Len    : 209     Alloc Len   : 209

TLVs :
Area Addresses :
  Area Address : (01) 00
  Area Address : (03) 00.00.00
Supp Protocols :
  Protocols    : SPB
IS-Hostname    :
  Hostname     : Ix-SPB-4
TE IS Neighbors :
  Neighbor     : 0000.beb4.0006  SPB Metric 10 Num of Ports 1 Port-Id 0x1
  Neighbor     : e8e7.3233.199d  SPB Metric 10 Num of Ports 1 Port-Id 0x1
MT Capability   :
  MT-ID        : 0x0
  SPB INSTANCE :
    CIST Root-ID: 0x0 0x0
    CIST Ext Root Path Cost: 0x00000000  Bridge Priority: 0x8003
    SPSourceID: 0x001055f2 (Auto)        Number of Trees: 4
    [#1 ]ECT-algo:0x0080c201 baseVid:4001 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
    [#2 ]ECT-algo:0x0080c202 baseVid:4002 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
    [#3 ]ECT-algo:0x0080c203 baseVid:4003 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
    [#4 ]ECT-algo:0x0080c204 baseVid:4004 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
SPB SVCID-UCAST-ADDR :
  B-MAC 00.00.bc.b4.00.01 Base-VID 4001
  [ISID# 1] 1000 (T=0/R=0)
SPB SVCID-UCAST-ADDR :
  B-MAC 00.00.bc.b4.00.01 Base-VID 4002
  [ISID# 1] 1500 (T=0/R=0)
SPB SVCID-UCAST-ADDR :
  B-MAC 00.00.bc.b4.00.01 Base-VID 4003
  [ISID# 1] 2000 (T=0/R=0)
SPB SVCID-UCAST-ADDR :
  B-MAC 00.00.bc.b4.00.01 Base-VID 4004
  [ISID# 1] 2500 (T=0/R=0)

```

Release History

Release 7.3.1; command was introduced.

Related Commands**show spb isis adjacency**

Displays information about the ISIS-SPB adjacencies created for the SPB bridge.

show spb isis nodes

Displays the discovered node-level parameter values for all of the ISIS-SPB bridges participating in the topology.

MIB Objects

N/A

show spb isis nodes

Displays the discovered node-level parameter values for all of the ISIS-SPB switches participating in the topology.

show spb isis nodes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays the system name, system ID, SPsource ID, and bridge priority parameter values for the bridges discovered within the ISIS-SPB topology.

Examples

```
-> show spb isis nodes
```

```
SPB ISIS Nodes:
```

System Name	System Id	SourceID	BridgePriority
Bridge-1	00e0.b1e7.0188	0x70188	32768 (0x8000)
Bridge-2	00e0.b1e7.0bd3	0x70bd3	32768 (0x8000)
Bridge-4	e8e7.3233.2a1d	0x02a1d	32768 (0x8000)
Bridge-5	e8e7.3233.1891	0x31891	32768 (0x8000)
Bridge-6	e8e7.3233.199d	0x3199d	32768 (0x8000)
Bridge-7	e8e7.3233.1a29	0x31a29	32768 (0x8000)
Bridge-8	e8e7.3233.1c81	0x31c81	32768 (0x8000)

output definitions

System Name	The system name assigned to the SPB bridge.
System Id	The system ID of the SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
SourceID	The shortest path (SP) source ID value for the SPB bridge. This value identifies the source of multicast frames and is relevant only in the multicast tandem replication mode.
BridgePriority	The bridge priority value assigned to the SPB bridge.

Release History

Release 7.3.1; command was introduced.

Related Commands**show spb isis adjacency**

Displays information about the ISIS-SPB adjacencies created for the SPB bridge.

show spb isis info

Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis unicast-table

Displays the unicast forwarding information for the specified BVLANs. Use this command to verify unicast addresses were learned correctly on each SPB switch in the ISIS-SPB backbone topology.

show spb isis unicast-table [**bvlan** *bvlan_id*]

Syntax Definitions

bvlan_id The VLAN ID of an existing BVLAN.

Defaults

By default, the forwarding information for all BVLANs in the SPB topology is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **bvlan** *bvlan_id* parameter to display information for a specific BVLAN.

Examples

```
-> show spb isis unicast-table
SPB ISIS Unicast MAC Table:
```

BVLAN	Destination (Name : MAC Address)	Outbound Interface
4001	BRIDGE-2 : 00:e0:b1:e7:0b:d3	1/1
4001	BRIDGE-4 : e8:e7:32:00:2a:1d	1/1
4001	BRIDGE-5 : e8:e7:32:33:18:91	1/3
4001	BRIDGE-6 : e8:e7:32:33:19:9d	1/1
4001	BRIDGE-7 : e8:e7:32:33:1a:29	1/2
4001	BRIDGE-8 : e8:e7:32:33:1c:81	1/1
4002	BRIDGE-2 : 00:e0:b1:e7:0b:d3	1/1
4002	BRIDGE-4 : e8:e7:32:00:2a:1d	1/3
4002	BRIDGE-5 : e8:e7:32:33:18:91	1/3
4002	BRIDGE-6 : e8:e7:32:33:19:9d	1/2
4002	BRIDGE-7 : e8:e7:32:33:1a:29	1/2
4002	BRIDGE-8 : e8:e7:32:33:1c:81	1/3
4003	BRIDGE-2 : 00:e0:b1:e7:0b:d3	1/1
4003	BRIDGE-4 : e8:e7:32:00:2a:1d	1/3
4003	BRIDGE-5 : e8:e7:32:33:18:91	1/3
4003	BRIDGE-6 : e8:e7:32:33:19:9d	1/3
4003	BRIDGE-7 : e8:e7:32:33:1a:29	1/2
4003	BRIDGE-8 : e8:e7:32:33:1c:81	1/3
4004	BRIDGE-2 : 00:e0:b1:e7:0b:d3	1/1
4004	BRIDGE-4 : e8:e7:32:00:2a:1d	1/1
4004	BRIDGE-5 : e8:e7:32:33:18:91	1/3
4004	BRIDGE-6 : e8:e7:32:33:19:9d	1/1
4004	BRIDGE-7 : e8:e7:32:33:1a:29	1/2
4004	BRIDGE-8 : e8:e7:32:33:1c:81	1/1

```

MAC Addresses: 24
-> show spb isis unicast-table bvlan 4001
SPB ISIS Unicast MAC Table:
      Destination                               Outbound
  BVLAN  (Name : MAC Address)                   Interface
-----+-----+-----+-----+-----+-----+-----+-----+-----+
  4001  BRIDGE-2                               : 00:e0:b1:e7:0b:d3    1/1
  4001  BRIDGE-4                               : e8:e7:32:00:2a:1d    1/1
  4001  BRIDGE-5                               : e8:e7:32:33:18:91    1/3
  4001  BRIDGE-6                               : e8:e7:32:33:19:9d    1/1
  4001  BRIDGE-7                               : e8:e7:32:33:1a:29    1/2
  4001  BRIDGE-8                               : e8:e7:32:33:1c:81    1/1

```

MAC Addresses: 6

output definitions

BVLAN	The VLAN ID number for the SPB BVLAN.
System (Name : BMAC)	The system name of the destination SPB bridge, and the destination unicast BMAC address for that bridge.
Outbound Interface	The interface (port or link aggregate) on which the destination system is reached.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis bvlans	Displays status and configuration information for the SPB instance.
show spb isis multicast-table	Displays the multicast forwarding information for the specified service instance identifier (I-SID).

MIB Objects

N/A

show spb isis services

Displays the service instance identifier (I-SID) mapping for bridges participating in the SPB topology. This command provides a network-wide view of existing services to help verify that SPB services are correctly advertised and learned by ISIS-SPB.

show spb isis services [*isis service_id* | *bvlan bvlan_id*]

Syntax Definitions

service_id An existing I-SID number.

bvlan_id The VLAN ID of an existing BVLAN.

Defaults

By default, the mapping for all I-SIDs in the SPB topology is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **isis** *service_id* number to display information for a specific service instance.
- Use the **bvlan** *bvlan_id* parameter to display information for a specific BVLAN.

Examples

```
-> show spb isis services
```

Legend: * indicates locally configured ISID

SPB ISIS Services Info:

ISID	BVLAN	System (Name : BMAC)	MCAST(T/R)
* 1000	4001	BRIDGE-1	: 00:e0:b1:e7:01:88
* 1000	4001	BRIDGE-4	: e8:e7:32:00:2a:1d
* 1001	4001	BRIDGE-1	: 00:e0:b1:e7:01:88
* 1001	4001	BRIDGE-4	: e8:e7:32:00:2a:1d
* 1002	4001	BRIDGE-1	: 00:e0:b1:e7:01:88
* 1002	4001	BRIDGE-4	: e8:e7:32:00:2a:1d
* 1003	4001	BRIDGE-1	: 00:e0:b1:e7:01:88
* 1003	4001	BRIDGE-4	: e8:e7:32:00:2a:1d
* 1004	4001	BRIDGE-1	: 00:e0:b1:e7:01:88
* 1004	4001	BRIDGE-4	: e8:e7:32:00:2a:1d
* 1005	4001	BRIDGE-1	: 00:e0:b1:e7:01:88
* 1005	4001	BRIDGE-4	: e8:e7:32:00:2a:1d
* 1006	4001	BRIDGE-1	: 00:e0:b1:e7:01:88
* 1006	4001	BRIDGE-4	: e8:e7:32:00:2a:1d
* 1007	4001	BRIDGE-1	: 00:e0:b1:e7:01:88
* 1007	4001	BRIDGE-4	: e8:e7:32:00:2a:1d

ISIDs: 16

output definitions

ISID	The service instance identifier.
BVLAN	The VLAN ID number for the SPB BVLAN.
System (Name : BMAC)	The system name of the SPB bridge from where the I-SID was discovered or configured, and the destination unicast BMAC address to which frames associated with the service instance are sent.
Multicast (T/R)	Indicates the multicast service requirement for the instance (T ransmit, R ecieve, or both).

Release History

Release 7.3.1; command was introduced.

Related Commands

[show spb isis info](#) Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis spf

Displays the shortest path first (SPF) information to all known SPB bridges for a specific BVLAN.

```
show spb isis spf bvlan bvlan_id [bmac mac_address]
```

Syntax Definitions

bvlan_id The VLAN ID of an existing BVLAN.

mac_address An SPB bridge BMAC address.

Defaults

By default, the SPF information for all known BMAC addresses for the specified BVLAN.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **bmac** *mac_address* parameter to display information for a specific SPB bridge.

Examples

```
-> show spb isis spf bvlan 4001
```

```
SPB ISIS Path Table:
```

Destination (Name : BMAC)	Outbound Interface	Next Hop (Name : BMAC)	SPB Metric	Num Hops
BRIDGE-1 : 00:e0:b1:e7:01:88	1/3	BRIDGE-2 : 00:e0:b1:e7:0b:d3	20	2
BRIDGE-2 : 00:e0:b1:e7:0b:d3	1/3	BRIDGE-2 : 00:e0:b1:e7:0b:d3	10	1
BRIDGE-4 : e8:e7:32:00:2a:1d	1/2	BRIDGE-4 : e8:e7:32:00:2a:1d	10	1
BRIDGE-5 : e8:e7:32:33:18:91	1/1	BRIDGE-5 : e8:e7:32:33:18:91	10	1
BRIDGE-6 : e8:e7:32:33:19:9d	1/3	BRIDGE-2 : 00:e0:b1:e7:0b:d3	20	2
BRIDGE-7 : e8:e7:32:33:1a:29	1/3	BRIDGE-2 : 00:e0:b1:e7:0b:d3	30	3

```
SPF Path count: 6
```

```
-> show spb isis spf bvlan 4001 bmac e8:e7:32:33:1a:29
```

```
SPB ISIS Path Details:
```

Path Hop Name	Path Hop BMAC
BRIDGE-7	e8:e7:32:33:1a:29
BRIDGE-1	00:e0:b1:e7:01:88
BRIDGE-2	00:e0:b1:e7:0b:d3

output definitions

Destination (Name : BMAC)	The system name of the destination SPB bridge, and the destination BMAC address for that bridge.
Outbound Interface	The interface (port or link aggregate) on which the destination system is reached.

output definitions (continued)

Next Hop (Name : BMAC)	The system name of the next-hop SPB bridge, and the BMAC address for that bridge.
SPB Metric	The metric (cost) to reach the destination BMAC address.
Num Hops	The number of hops along the path to the destination.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis multicast-sources-spf	Displays the SPF reachability for a known multicast source bridge for a specific BVLAN.
show spb isis info	Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis multicast-table

Displays the multicast forwarding information for the specified service instance identifier (I-SID).

show spb isis multicast-table [*isid service_id*]

Syntax Definitions

service_id An existing I-SID number.

Defaults

By default, the forwarding information for all services in the SPB topology is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **isid** *service_id* parameter to display information for a specific service instance.

Examples

```
-> show spb isis multicast-table
SPB ISIS Multicast MAC Table:
```

ISID	BVLAN	MCAST Group Address	MCAST Source (Name:BMAC)	Inbound Interface	Outbound Interface
2000	41	0a:fd:c2:00:01:22	BRIDGE-8 : 00:d0:95:0a:fd:c2	1/2	1/3

MAC Addresses: 1

output definitions

ISID	The service instance identifier.
BVLAN	The VLAN ID number for the SPB BVLAN associated with the service instance.
MCAST Group Address	The multicast destination group address.
MCAST Source (Name : BMAC)	The system name and BMAC address of the multicast source.
Inbound Interface	The interface (port or link aggregate) on which multicast traffic is received for the service instance.
Outbound Interface	The interface (port or link aggregate) on which multicast traffic is sent for the service instance.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis multicast-sources Displays all the known multicast sources across the SPB domain and BVLANS.

show spb isis multicast-sources-spf Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.

MIB Objects

N/A

show spb isis multicast-sources

Displays all the known multicast sources across the SPB domain and BVLANS.

show spb isis multicast-sources

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command also displays whether or not the source is reachable.

Examples

```
-> show spb isis multicast-sources
SPB ISIS Multicast Source Nodes:
Multicast Source
(Name : BMAC)                Reachable   (# ) BVIDS
-----+-----+-----
BRIDGE-8   : 00:d0:95:0a:fd:c2   YES        (#2) 4001 4002

Total SPB Multicast Source Nodes: 1
```

output definitions

Multicast Source (Name : BMAC)	The system name and BMAC address of the multicast source bridge.
Reachable	Indicates whether or not the multicast source node is reachable (YES or NO).
(#) BVIDS	Indicates the number of BVLANS and the BVLAN IDs on which the bridge acts as a multicast source.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis multicast-sources-spf

Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.

show spb isis multicast-table

Displays the multicast forwarding information for the specified service instance identifier (I-SID).

show spb isis info

Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis multicast-sources-spf

Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.

show spb isis multicast-sources-spf *bvlan* *bvlan_id* **bmac** *mac_address* [**dest** *mac_address*]

Syntax Definitions

bvlan_id The VLAN ID of an existing BVLAN.

mac_address An SPB bridge BMAC address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **dest** *mac_address* parameter to display information for a specific SPB bridge.

Examples

```
-> show spb isis multicast-sources-spf bvlan 4001 bmac 00:d0:95:0a:fd:c2
SPB ISIS Path Table:
Destination                               Outbound Next Hop                               SPB      Num
(Name : BMAC)                             Interface (Name : BMAC)                         Metric  Hops
-----+-----+-----+-----+-----+-----
BRIDGE-1 : 00:d0:95:03:19:12             1/1   BRIDGE-7 : 00:d0:95:09:79:02             30      3
BRIDGE-2 : 00:d0:95:06:4c:62             1/1   BRIDGE-7 : 00:d0:95:09:79:02             20      2
BRIDGE-3 : 00:d0:95:07:97:32             1/1   BRIDGE-7 : 00:d0:95:09:79:02             20      2
BRIDGE-6 : 00:d0:95:08:f2:12             1/2   BRIDGE-6 : 00:d0:95:08:f2:12             10      1
BRIDGE-7 : 00:d0:95:09:79:02             1/1   BRIDGE-7 : 00:d0:95:09:79:02             10      1
```

SPF Path count: 5

```
-> show spb isis spf bvlan 4001 bmac 00:d0:95:0a:fd:c2 dest 00:d0:95:03:19:12
SPB ISIS Multicast Source Path Details:
Path Hop Name                             Path Hop BMAC
-----+-----+-----+-----+-----
BRIDGE-1                                 00:d0:95:03:19:12
BRIDGE-3                                 00:d0:95:07:97:32
BRIDGE-7                                 00:d0:95:09:79:02
```

output definitions

Destination (Name : BMAC)	The system name and BMAC address of the destination SPB bridge.
Outbound Interface	The interface (port or link aggregate) on which the destination system is reached.

output definitions (continued)

Next Hop (Name : BMAC)	The system name and BMAC address of the next-hop SPB bridge.
SPB Metric	The metric (cost) to reach the destination BMAC address.
Num Hops	The number of hops along the path to the destination.

Release History

Release 7.3.1; command was introduced.

Related Commands

show spb isis multicast-sources	Displays all the known multicast sources across the SPB domain and BVLANS.
show spb isis multicast-table	Displays the multicast forwarding information for the specified service instance identifier (I-SID).
show spb isis spf	Displays the SPF information to all known SPB bridges for a specific BVLAN.
show spb isis info	Displays status and configuration information for the SPB instance

MIB Objects

N/A

show spb isis ingress-mac-filter

Displays the ingress MAC filter for multicast traffic for a given BVLAN operating in the (*,G) mode.

show spb isis ingress-mac-filter [**port** *slot/port*[-*port2*] | **linkagg** *agg_id*[-*agg_id2*] | **bvlan** *bvlan_id* | **bmac** *mac_address*]

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i> [- <i>agg_id2</i>]	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
<i>bvlan_id</i>	The VLAN ID of an existing BVLAN.
<i>mac_address</i>	The source MAC address of the multicast traffic allowed on the specified BVLAN and physical port.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the optional command parameters to display specific information with this command.
- Each of the optional command parameters can be combined with any of the other optional parameters within the same command line.

Examples

```
-> show spb isis ingress-mac-filter
SPB ISIS Ingress MAC Table (for GMODE bvlan only):
      Inbound      Multicast source MAC
      BVLAN  Interface  (Name : MAC Address)
-----+-----+-----
      40      1/1      BRIDGE-1           : 00:d0:95:04:8d:92
```

MAC Addresses: 1

output definitions

BVLAN	The VLAN ID number for the SPB BVLAN.
Inbound Interface	The interface (port or link aggregate) on which the multicast source MAC was received.
System (Name : BMAC)	The system name and MAC address of the multicast traffic source.

Release History

Release 7.3.1; command was introduced.

Related Commands

[show spb isis info](#)

Displays status and configuration information for the SPB instance

MIB Objects

N/A

8 Link Aggregation Commands

Link aggregation combines 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	linkagg static agg size linkagg static agg name linkagg static agg admin-state linkagg static port agg
Dynamic link aggregates	linkagg lacp agg size linkagg lacp agg name linkagg lacp agg admin-state linkagg lacp agg actor admin-key linkagg lacp agg actor system-priority linkagg lacp agg actor system-id linkagg lacp agg partner system-id linkagg lacp agg partner system-priority linkagg lacp agg partner admin-key linkagg lacp port actor admin-key linkagg lacp port actor admin-state linkagg lacp port actor system-id linkagg lacp port actor system-priority linkagg lacp agg partner admin-state linkagg lacp port partner admin system-id linkagg lacp port partner admin-key linkagg lacp port partner admin system-priority linkagg lacp port actor port priority linkagg lacp port partner admin-port linkagg lacp port partner admin port-priority
Static and dynamic	linkagg range show linkagg range show linkagg show linkagg port

linkagg static agg size

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

linkagg static agg *agg_num1* [-*agg_num2*] **size** *size* [**name** *name*] [**admin-state** {**enable** | **disable**}] [**multi-chassis active**] [**hash** (**source-mac** | **destination-mac** | **source-and-destination-mac** | **source-ip** | **destination-ip** | **source-and-destination-ip**)]

no linkagg static agg *agg_num1* [-*agg_num2*]

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the static aggregate group.
<i>-agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>size</i>	The maximum number of links allowed in the aggregate group.
<i>name</i>	The name of the static aggregate group. Can be any alphanumeric string. Spaces must be contained 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.
multi-chassis active	Specifies that the multi-chassis link aggregate feature should be activated on the static aggregate group between the two switches.
source-mac	Selects the source MAC address hashing option.
destination-mac	Selects the destination MAC address hashing option.
source-and-destination-mac	Selects the source MAC address and destination MAC address hashing option.
source-ip	Selects the source IP hashing option.
destination-ip	Selects the destination IP hashing option.
source-and-destination-ip	Selects the source IP and destination IP hashing option.

Defaults

parameter	default
enable disable	enable
<i>hash_option</i>	source-and-destination-IP (Layer 3 traffic) source-and-destination-mac (Layer 2 traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a static aggregate group or a range of static aggregate groups from the configuration.
- If the static aggregate has any attached ports you must delete the attached ports with the **no** form of the **linkagg static port agg** command before you remove the static link aggregate ID. Delete the attached ports using the **no linkagg static port** command.
- Use the **multi-chassis active** parameter to activate a static link aggregate group between multiple switch chassis. This parameter is used only in a multi-chassis link aggregation (MC-LAG) configuration.
- Specify the **hash** parameter option when the link aggregate is first created. The hashing algorithm options apply to unicast traffic and are not modifiable once the aggregate is created. If different options are required:
 - Disassociate all ports currently associated with the aggregate.
 - Delete the aggregate from the switch configuration.
 - Create the aggregate again with the new hashing options.
- It is not necessary to administratively down the linkagg ports before changing the hashing algorithm, but doing so is recommended.
- The hashing algorithm does not take into consideration the speed of the ports to distribute the traffic. In other words, the same number of flows is distributed evenly on each port without consideration of the line speed.
- Aggregate load balancing is performed at the ingress side.
- Per-aggregate hashing is local to the switch, so each side of the aggregation can use different configurations for the hashing algorithms.
- Link aggregation follows the global hash control settings configured through the **hash-control brief** or **hash-control extended** commands.
- For example, if the **source-mac** option is specified for L2 hashing:
 - If the global hash-control is in brief mode, hashing is based on source MAC address only.
 - If the global hash-control is in extended mode, hashing is based on source MAC address, VLAN, Ethertype, and source module ID/port.
- For example, if the **source-ip** option is specified for L3 hashing:
 - If the global hash-control is in brief mode, hashing is based on source IP address only.
 - If the global hash-control is in extended mode, hashing is based on source IP address and source UDP-TCP Port.
- To load balance Unknown Destination/Broadcast/Multicast traffic on all the ports of the aggregate, use the **hash-control** command to enable load balancing of DFL traffic.
- Use the **linkagg lacp agg size** command to create a dynamic aggregation (LACP) group.

Examples

```
-> linkagg static agg 3-10 size 8
-> linkagg static agg 4 size 2 admin-state disable
-> linkagg static agg 4 size 2 multichassis-active
-> linkagg static agg 4 size 2 hash source-and-destination-ip
-> no linkagg static agg 3-10
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show linkagg](#)

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

MIB Objects

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

linkagg static agg name

Configures a name for an existing static aggregate group.

linkagg static agg *agg_num1* [-*agg_num2*] **name** *name*

no linkagg static agg *agg_num1* [-*agg_num2*] **name**

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the static aggregate group.
<i>-agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>name</i>	The name of the static aggregation group, can be an alphanumeric string. Spaces must be contained within quotes (for example, "Static Group 1").

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a name from a static aggregate or from a range of static aggregates.
- You must assign names to static link aggregate IDs individually.
- To specify a range of link aggregates, use hyphen between the first and last link aggregate IDs of the range. A range of link aggregate IDs can be used only with the **no** form of this command.

Examples

```
-> linkagg static agg 2 name accounting  
-> no linkagg static agg 2-10 name
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg static agg size](#)

Creates a static aggregate group.

[show linkagg](#)

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

MIB Objects

alclnkaggAggTable

alclnkaggAggNumber

alclnkaggAggName

linkagg static agg admin-state

Enables or disables the administrative state of a static link aggregation group.

linkagg static agg *agg_num1*[-*agg_num2*] **admin-state** {**enable** | **disable**}

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the static aggregate group.
- <i>agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
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 10K, 6900

Usage Guidelines

When the administrative state is set to **disable**, the static aggregate group is disabled.

Examples

```
-> linkagg static agg 2 admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
  alclnkaggAggNumber
  alclnkaggAggAdminState
```

linkagg static port agg

Configures a slot and port for a static aggregate group.

linkagg static port *slot/port[-port2]* **agg** *agg_num*

no linkagg static port *slot/port[-port2]*

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>agg_num</i>	The number corresponding to the static aggregate group.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove one or more ports from a static aggregate group.
- A port can belong to only one aggregate group.
- Ports that belong to the same static aggregate group need not be configured sequentially and can be on any Network Interface (NI).
- To specify a range of link aggregates, use hyphen between the first and last link aggregate IDs of the range. A range of link aggregate IDs can be used only with the **no** form of this command.

Examples

```
-> linkagg static port 2/1-5 agg 4  
-> no linkagg static port 2/1-5
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static agg size

Creates a static aggregate group.

show linkagg port

Displays information about link aggregation ports.

MIB Objects

alclnkaggAggPortTable

alclnkaggAggPortGlobalPortNumber

alclnkaggAggPortLacpType

alclnkaggAggPortSelectedAggNumber

linkagg lacp agg 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.

```
linkagg lacp agg agg_num1 [-agg_num2] size size
  [name name]
  [admin-state {enable | disable}]
  [actor admin-key actor_admin_key]
  [actor system-priority actor_system_priority]
  [actor system-id actor_system_id]
  [partner system-id partner_system_id]
  [partner system-priority partner_system_priority]
  [partner admin-key partner_admin_key]
  [multi-chassis active]
  [hash (source-mac | destination-mac | source-and-destination-mac | source-ip | destination-ip |
source-and-destination-ip)]
```

```
no linkagg lacp agg agg_num1 [-agg_num2] size size
```

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the dynamic aggregate group.
<i>-agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>size</i>	The maximum number of links that can belong to the aggregate.
<i>name</i>	The name of the dynamic aggregate group. can be an alphanumeric string. 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.
<i>actor_admin_key</i>	The administrative key value associated with the dynamic aggregate group.
<i>actor_system_priority</i>	The priority of the dynamic aggregate group.
<i>actor_system_id</i>	The MAC address of the dynamic aggregate group on the switch.
<i>partner_system_id</i>	The MAC address of the aggregate group of the remote system which is attached to the aggregate group of the switch.
<i>partner_system_priority</i>	The priority of the remote system to which the aggregation group is attached.
<i>partner_admin_key</i>	The administrative key for the remote partner of the aggregation group.
multi-chassis active	Specifies that the multi-chassis link aggregate feature should be activated on the dynamic aggregate group between the two switches.

source-mac	Selects the source MAC address hashing option.
destination-mac	Selects the destination MAC address hashing option.
source-and-destination-mac	Selects the source MAC address and destination MAC address hashing option.
source-ip	Selects the source IP hashing option.
destination-ip	Selects the destination IP hashing option.
source-and-destination-ip	Selects the source IP and destination IP hashing option.

Defaults

parameter	default
enable disable	enable
<i>hash_option</i>	source-and-destination-IP (Layer 3 traffic) source-and-destination-mac (Layer 2 traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a dynamic aggregate group from the configuration.
- You must disable the group with the **linkagg lacp agg admin-state** command before you can delete a dynamic link aggregate group.
- Optional parameters for the dynamic aggregate group can be configured when the aggregate is created. The dynamic aggregate group can be modified after the optional parameters are assigned.
- Use the **multi-chassis active** parameter to activate a dynamic link aggregate group between multiple switch chassis. This parameter is used only in a multi-chassis link aggregation (MC-LAG) configuration.
- Specify the **hash** parameter option when the link aggregate is first created. The hashing algorithm options apply to unicast traffic and are not modifiable once the aggregate is created. If different options are required:
 - Disassociate all ports currently associated with the aggregate.
 - Delete the aggregate from the switch configuration.
 - Create the aggregate again with the new hashing options.
- It is not necessary to administratively down the linkagg ports before changing the hashing algorithm, but doing so is recommended.
- The hashing algorithm does not take into consideration the speed of the ports to distribute the traffic. In other words, the same number of flows is distributed evenly on each port without consideration of the line speed.
- Aggregate load balancing is performed at the ingress side.

- Per-aggregate hashing is local to the switch, so each side of the aggregation can use different configurations for the hashing algorithms.
- Link aggregation follows the global hash control settings configured through the **hash-control brief** or **hash-control extended** commands.
- For example, if the **source-mac** option is specified for L2 hashing:
 - If the global hash-control is in brief mode, hashing is based on source MAC address only.
 - If the global hash-control is in extended mode, hashing is based on source MAC address, VLAN, Ethertype, and source module ID/port.
- For example, if the **source-ip** option is specified for L3 hashing:
 - If the global hash-control is in brief mode, hashing is based on source IP address only.
 - If the global hash-control is in extended mode, hashing is based on source IP address and source UDP-TCP Port.
- To load balance Unknown Destination/Broadcast/Multicast traffic on all the ports of the aggregate, use the **hash-control** command to enable load balancing of DFL traffic.
- Use the **linkagg static agg size** command to create static aggregate groups. See [page 8-3](#) for more information about this command.

Examples

```
-> linkagg lacp agg 2-5 size 4
-> linkagg lacp agg 3 size 2 admin-state disable actor system-priority 65535
-> no linkagg lacp agg 2-5 size 4
```

Release History

Release 7.1.1; 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
```

linkagg lacp agg name

Configures a name for a dynamic aggregate group.

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

no linkagg lacp agg *agg_num1* [-*agg_num2*] **name**

Syntax Definitions

<i>agg_num</i>	The number corresponding to the dynamic aggregate group.
<i>-agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>name</i>	The name of the dynamic aggregate group. Can be an alphanumeric string. Spaces must be contained within quotes (for example, "Dynamic Group 1").

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a name from a single or a range of dynamic aggregate groups simultaneously.
- Assign names to individual dynamic link aggregate groups separately.

Examples

```
-> linkagg lacp agg 2 name finance  
-> no linkagg lacp agg 2-5 name
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg size](#)

Creates a dynamic aggregate group.

[show linkagg](#)

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

MIB Objects

alclnkaggAggTable

alclnkaggAggNumber

alclnkaggAggName

linkagg lacp agg admin-state

Configures the administrative state of a dynamic aggregate group or a range of dynamic aggregate groups.

linkagg lacp agg *agg_num1* [-*agg_num2*] **admin-state** {**enable** | **disable**}

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the dynamic aggregate group.
<i>-agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
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 10K, 6900

Usage Guidelines

- When the administrative state is set to **disable**, the operation of a dynamic aggregation (LACP) group cannot be performed.
- You can also enable or disable the admin-state for a range of link aggregate IDs simultaneously, using this command.

Examples

```
-> linkagg lacp agg 2 admin-state disable  
-> linkagg lacp agg 2-10 admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size

Creates a dynamic aggregate group.

show linkagg

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

show linkagg port

Displays information about ports associated with a particular aggregate group or all aggregates.

MIB Objects

alclnkaggAggTable
 alclnkaggAggNumber
 alclnkaggAggAdminState

linkagg lacp agg actor admin-key

Configures the administrative key associated with a dynamic aggregate group.

linkagg lacp agg *agg_num1* [-*agg_num2*] **actor admin-key** *actor_admin_key*

no linkagg lacp agg *agg_num1* [-*agg_num2*] **actor admin-key**

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the dynamic aggregate group.
- <i>agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>actor_admin_key</i>	The administrative key value associated with the dynamic aggregate group.

Defaults

parameter	default
<i>actor_admin_key</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to remove an actor admin key from a dynamic aggregate group.

Examples

```
-> linkagg lacp agg 3-5 actor admin-key 2
-> no linkagg lacp agg 3-5 actor admin-key
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg size	Creates a dynamic aggregate group.
show linkagg	Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
  alclnkaggAggNumber
  alclnkaggAggActorAdminKey
```

linkagg lacp agg actor system-priority

Configures the priority of the dynamic aggregate group.

linkagg lacp agg *agg_num1* [-*agg_num2*] **actor system-priority** *actor_system_priority*

no linkagg lacp agg *agg_num1* [-*agg_num2*] **actor system-priority**

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the link aggregate group.
- <i>agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>actor_system_priority</i>	The priority of the dynamic aggregate group of the switch in relation to other aggregate groups.

Defaults

parameter	default
<i>actor_system_priority</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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.
- To assign or remove the actor system-priority for a series of link aggregate IDs, specify the range of link aggregate IDs with the **agg** keyword. Use a hyphen to separate the first and last link aggregate IDs of a range.

Examples

```
-> lacp linkagg 3 actor system-priority 100
-> no lacp linkagg 3 actor system-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg size](#)

Creates a dynamic aggregate group.

[show linkagg](#)

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

MIB Objects

alclnkaggAggTable

alclnkaggAggNumber

alclnkaggAggActorSystemPriority

linkagg lacp agg actor system-id

Configures the MAC address of a dynamic aggregate group on the switch.

```
linkagg lacp agg agg_num1 [-agg_num2] actor system-id actor_system_id
```

```
no linkagg lacp agg agg_num1 [-agg_num2] actor system-id
```

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the dynamic aggregate group.
- <i>agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>actor_system_id</i>	The MAC address of the dynamic aggregate group on the switch in the hexadecimal format <i>xx:xx:xx:xx:xx:xx</i> .

Defaults

parameter	default
<i>actor_system_id</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the MAC address assignment (actor system ID) from a dynamic link aggregate or a range of dynamic link aggregates simultaneously.
- You can configure the MAC address for a range of dynamic link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range along with this command.

Examples

```
-> linkagg lacp agg 2 actor system-id 00:20:da:81:d5:b0  
-> no linkagg lacp agg 3-10 actor system-id  
-> no linkagg lacp agg 11 actor system-id
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg size](#)

Creates a dynamic aggregate group.

[show linkagg](#)

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

MIB Objects

alclnkaggAggTable

alclnkaggAggNumber

alclnkaggAggActorSystemID

linkagg lacp agg partner system-id

Configures the MAC address of the dynamic aggregate group of the remote system that is attached to the dynamic aggregate group of the local switch.

linkagg lacp agg *agg_num1* [-*agg_num2*] **partner system-id** *partner_system_id*

no linkagg lacp agg *agg_num1* [-*agg_num2*] **partner system-id**

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the dynamic aggregate group on the switch.
- <i>agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>partner_system_id</i>	The MAC address of the dynamic aggregate group of the remote switch in the hexadecimal format <i>xx:xx:xx:xx:xx:xx</i> .

Defaults

parameter	default
<i>partner_system_id</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a partner system ID from a dynamic aggregate group or a range of groups assigned with the same partner system IDs together.
- The *partner_system_id* and the *partner_system_priority* together specify the priority of the remote system.
- You can configure a partner system ID for a range of dynamic link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range along with this command.

Examples

```
-> linkagg lacp agg 2 partner system-id 00:20:da4:32:81
-> linkagg lacp agg 2-10 partner system-id 00:20:da4:32:82
-> no linkagg lacp agg 2-10 partner system-id
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg size](#)

Creates a dynamic aggregate group.

[show linkagg](#)

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

MIB Objects

alclnkaggAggTable

alclnkaggAggNumber

alclnkaggAggPartnerSystemID

linkagg lacp agg partner system-priority

Configures the priority of the dynamic aggregate group of the remote system which is attached to the dynamic aggregate group of the local switch.

linkagg lacp agg *agg_num1* [-*agg_num2*] **partner system-priority** *partner_system_priority*

no linkagg lacp agg *agg_num1* [-*agg_num2*] **partner system-priority**

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the dynamic aggregate group.
<i>-agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>partner_system_priority</i>	The priority of the dynamic aggregate group of the remote system which is attached to the dynamic aggregate group of the local switch.

Defaults

parameter	default
<i>partner_system_priority</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to return to the priority value to its default.
- The *partner_system_id* and the *partner_system_priority* together specify the priority of the remote system.
- You can apply the partner system-priority to a range of link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range after the **agg** keyword.

Examples

```
-> linkagg lacp agg 3 partner system-priority 65535
-> linkagg lacp agg 3-6 partner system-priority 65535
-> no linkagg lacp agg 3-6 partner system-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg size](#)

Creates a dynamic aggregate group.

[show linkagg](#)

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

MIB Objects

alclnkaggAggTable

alclnkaggAggNumber

alclnkaggAggPartnerSystemPriority

linkagg lacp agg partner admin-key

Configures the administrative key for the remote partner of the dynamic aggregation group.

```
linkagg lacp agg agg_num1[-agg_num2] partner admin-key partner_admin_key
```

```
no linkagg lacp agg agg_num1[-agg_num2] partner admin-key
```

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the dynamic aggregate group.
- <i>agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>partner_admin_key</i>	The administrative key for the remote partner of the dynamic aggregation group.

Defaults

parameter	default
<i>partner_admin_key</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a partner admin-key from a dynamic aggregate group.
- The partner admin-key can be assigned for a range of dynamic link aggregate IDs simultaneously.

Examples

```
-> linkagg lacp agg 3-5 partner admin-key 3  
-> no linkagg lacp agg 3-10 partner admin-key
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg size](#)

Creates a dynamic aggregate group.

[show linkagg](#)

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

MIB Objects

alclnkaggAggTable

alclnkaggAggNumber

alclnkaggAggPartnerAdminKey

linkagg lacp port actor admin-key

Configures an actor administrative key for a port, which allows the port to join a dynamic aggregate group.

```
linkagg lacp port slot/port[-port2] actor admin-key actor_admin_key
  [actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default]
  [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 {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default]
  [expire] | none}]
  [actor port priority actor_port_priority]
  [partner admin port partner_admin_port]
  [partner admin port priority partner_admin_port_priority]

no linkagg lacp port slot/port[-port2] [actor admin-state {[active] [timeout] [aggregate] [synchronize]
[collect] [distribute] [default] [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 {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default]
  [expire] | none}]
  [actor port priority actor_port_priority]
  [partner admin port partner_admin_port]
  [partner admin port priority partner_admin_port_priority]
```

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of slot/port IDs.
<i>actor_admin_key</i>	The administrative key associated with this dynamic aggregate group.
actor admin-state	See the linkagg lacp port actor admin-state command.
<i>actor_system_id</i>	The MAC address of this dynamic aggregate group on the switch.
<i>actor_system_priority</i>	The priority of the dynamic aggregate group.
<i>partner_admin_system_id</i>	The MAC address of the dynamic aggregate group of the remote switch.

<i>partner_admin_key</i>	The administrative key for the remote partner of the dynamic aggregation group.
<i>partner_admin_system_priority</i>	The priority of the remote system to which the dynamic aggregation group is attached.
partner admin-state	See the linkagg lacp agg partner admin-state command.
<i>actor_port_priority</i>	The priority of the actor port.
<i>partner_admin_port</i>	The administrative state of the partner port.
<i>partner_admin_port_priority</i>	The priority of the partner port.

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a slot and port from a dynamic aggregate group.
- A port can belong to only one aggregate group.
- Ports that belong to a dynamic link aggregate must be configured to the same link speed.
- Ports that belong to the same dynamic aggregate group need not be configured sequentially and can be on any Network Interface (NI).

Examples

```
-> linkagg lacp agg 3/1 actor admin-key 0
-> no linkagg lacp agg 3/1 actor admin-key
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg 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
```

linkagg lacp port 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.

linkagg lacp port *slot/port*[-*port2*] actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}

no linkagg lacp port *slot/port*[-*port2*] actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
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 10K, 6900

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.

Examples

```
-> linkagg lacp port 4/2 actor admin-state synchronize collect distribute
-> no linkagg lacp port 4/2 actor admin-state synchronize collect
-> linkagg lacp port 4/2 actor admin-state none
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg 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
```

linkagg lacp port actor system-id

Configures the system ID (i.e., MAC address) for the local port associated with a dynamic aggregate group.

```
linkagg lacp port slot/port[-port2] actor system-id actor_system_id
```

```
no linkagg lacp port slot/port[-port2] actor system-id
```

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>actor_system_id</i>	The MAC address of the dynamic aggregate group on the switch in the hexadecimal format <i>xx:xx:xx:xx:xx:xx</i> .

Defaults

parameter	default
<i>actor_system_id</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the actor system ID from a slot and port or a range of slot and ports associated with a dynamic aggregate group.
- Configure the system ID for a range of local ports simultaneously. Use a hyphen to separate the first and last port IDs of a range after the **port** keyword.

Examples

```
-> linkagg lacp port 3/1-10 actor system-id 00:20:da:06:ba:d3  
-> no linkagg lacp port 3/1-10 actor system-id
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg 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

linkagg lacp port actor system-priority

Configures the system priority of the port on the switch that belongs to the dynamic aggregate group.

```
linkagg lacp port slot/port[-port2] actor system-priority actor_system_priority
```

```
no linkagg lacp port slot/port[-port2] actor system-priority
```

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>actor_system_priority</i>	The priority of the dynamic aggregate group.

Defaults

parameter	default
<i>actor_system_priority</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove an actor system priority value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.
- Configure the actor system-priority to a range of ports simultaneously. Use a hyphen to separate the first and last port of a range after the **port** keyword.

Examples

```
-> linkagg lacp port 3/2-10 actor system-priority 65  
-> no linkagg lacp port 3/2-10 actor system-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg 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

linkagg 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.

linkagg lacp port *slot/port*[-*port2*] partner admin-state
 {[**active**] [**timeout**] [**aggregate**] [**synchronize**] [**collect**] [**distribute**] [**default**] [**expire**] | **none**}

no linkagg lacp port *slot/port*[-*port2*] partner admin-state
 {[**active**] [**timeout**] [**aggregate**] [**synchronize**] [**collect**] [**distribute**]
 [**default**] [**expire**] | **none**}

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
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 10K, 6900

Usage Guidelines

- Use the **no** form of this command to restore the LACPDU bit settings to their default configuration for a single port or a range of ports.
- When the partner admin-state is set to **none**, all bit values are restored to their default configurations.
- Configure the system administrative state for a range of ports simultaneously. Use a hyphen to separate the first and last port of a range after the **port** keyword.

Examples

```
-> lacp port 4/2-10 partner admin-state synchronize collect distribute
-> no lacp agg 4/2-10 partner admin-state synchronize collect
```

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg lacp agg 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
```

linkagg lacp port partner admin system-id

Configures the partner administrative system ID for a dynamic aggregate group port.

linkagg lacp port *slot/port[-port2]* **partner admin system-id** *partner_admin_system_id*

no linkagg lacp port *slot/port[-port2]* **partner admin system-id**

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>partner_admin_system_id</i>	The MAC address of the remote dynamic aggregate group in the hexadecimal format <i>xx:xx:xx:xx:xx:xx</i> .

Defaults

parameter	default
<i>partner_admin_system_id</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to remove a partner administrative system ID from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 3/1-10 partner admin system-id 00:20:da:05:f6:23
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg 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

linkagg lacp port partner admin-key

Configures the partner administrative key for a dynamic aggregate group port.

```
linkagg lacp port slot/port[-port2] partner admin-key partner_admin_key
```

```
no linkagg lacp port slot/port[-port2] partner admin-key
```

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>partner_admin_key</i>	The administrative key for the remote partner of a dynamic aggregation group.

Defaults

parameter	default
<i>partner_admin_key</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a partner admin key value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 partner admin-key 0  
-> no linkagg lacp port 2/1-5 partner admin-key
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg size](#)

Creates a dynamic aggregate group.

[show linkagg port](#)

Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

AlcLnkAggAggPortTable

alclnkaggAggPortGlobalPortNumber

alclnkaggAggPortPartnerAdminKey

linkagg lacp port partner admin system-priority

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

```
linkagg lacp port slot/port[-port2] partner admin system-priority partner_admin_system_priority
```

```
no linkagg lacp port slot/port[-port2] partner admin system-priority
```

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>partner_admin_system_priority</i>	The priority of the dynamic aggregate group of the remote switch to which the aggregation group is attached.

Defaults

parameter	default
<i>partner_admin_system_priority</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to remove a *partner_system_priority* value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 partner admin system-priority 65  
-> no linkagg lacp port 2/1-5 partner admin system-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg 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

linkagg lacp port actor port priority

Configures the priority for an actor port.

```
linkagg lacp port slot/port[-port2] actor port-priority actor_port_priority
```

```
no linkagg lacp port slot/port[-port2] actor port-priority
```

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>actor_port_priority</i>	The priority of the actor port.

Defaults

parameter	default
<i>actor_port_priority</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to remove an *actor_port_priority* value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 actor port-priority 100  
-> no linkagg lacp port 2/1-5 actor port-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg 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

linkagg lacp port partner admin-port

Configures the administrative status of a partner port.

linkagg lacp port *slot/port[-port2]* **partner admin-port** *partner_admin_port*

no linkagg lacp port *slot/port[-port2]* **partner admin-port**

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>partner_admin_port</i>	The administrative state of the partner port.

Defaults

parameter	default
<i>partner_admin_port</i>	0

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to remove a *partner_admin_port* value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 partner admin-port 255
-> no linkagg lacp port 2/1-5 partner admin-port
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg 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

linkagg lacp port partner admin port-priority

Configures the priority for a partner port.

```
linkagg lacp port slot/port[-port2] partner admin port-priority partner_admin_port_priority
```

```
no linkagg lacp port slot/port[-port2] partner admin port-priority
```

Syntax Definitions

<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port that the switch initially uses as the Spanning Tree virtual port for this aggregate.
<i>-port2</i>	The last port number in a range of port IDs.
<i>partner_admin_port_priority</i>	The priority of the partner port.

Defaults

parameter	default
<i>partner_admin_port_priority</i>	0

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to remove a *partner_admin_port_priority* value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

Examples

```
-> linkagg lacp port 2/1-5 partner admin port-priority 100
-> no linkagg lacp port 2/1-5 partner admin port-priority
```

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg lacp agg size](#)

Creates a dynamic aggregate group.

[show linkagg port](#)

Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

AlcLnkAggAggPortTable

alclnkaggAggPortGlobalPortNumber

alclnkaggAggPortPartnerAdminPortPriority

linkagg range

Modifies the range of standard and MC-LAG link aggregation identifiers.

linkagg range local {*agg_num-agg_num* / none} **peer** {*agg_num-agg_num* / none} **multi-chassis** {*agg_num-agg_num* / none}

Syntax Definitions

<i>agg_num</i>	The first or last identifier in the range.
local	The range of standard local aggregate identifiers.
peer	The range of standard peer aggregate identifiers.
multi-chassis	The range of MC-LAG aggregate identifiers.
none	No aggregate identifiers range is specified.

Defaults

parameter	default
local	0-47
peer	48-95
multi-chassis	96-127

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command in conjunction with the MC-LAG feature to change the maximum number of MC-LAG link aggregates that can be configured.
- The switch must be rebooted for the ranges to take affect.
- The maximum number of combined standard and MC-LAG link aggregates is 128.

Examples

```
-> linkagg range local 0-9 peer 10-19 multi-chassis 20-127
-> linkagg range local none peer none multi-chassis 0-127
```

Release History

Release 7.1.1; command introduced.

Related Commands

show linkagg range Displays the link aggregate ranges.

MIB Objects

```
alclnkaggAggConfig
  alclnkAggLocalRangeOperMin
  alclnkAggLocalRangeOperMax
  alclnkAggLocalRangeConfiguredMin
  alclnkAggLocalRangeConfiguredMax
  alclnkAggPeerRangeOperMin
  alclnkAggPeerRangeOperMax
  alclnkAggPeerRangeConfiguredMin
  alclnkAggPeerRangeConfiguredMax
  alclnkAggMcLagRangeOperMin
  alclnkAggMcLagRangeOperMax
  alclnkAggMcLagRangeConfiguredMin
  alclnkAggMcLagRangeConfiguredMax
```

show linkagg

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

```
show linkagg {agg [agg_num1 [-agg_num2]}
```

Syntax Definitions

agg_num1 Specifies the aggregate group. Configured through the **linkagg static agg size** or **linkagg lacp agg size** command.

-agg_num2 The last link aggregate ID in a range of link aggregate IDs.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If no aggregation number is specified, information for all aggregate groups is displayed. If an aggregate number is specified, only the information about the relevant aggregate group is displayed. The fields included in the display depend on whether the aggregate group is a static or dynamic.
- Use the **show linkagg port** command to display information about aggregate group ports.

Examples

No aggregate group is specified:

```
-> show linkagg
```

Number	Aggregate	SNMP Id	Size	Admin State	Oper State	Att/Sel Ports
1	Static	40000001	8	ENABLED	UP	2 2
2	Dynamic	40000002	4	ENABLED	DOWN	0 0
3	Dynamic	40000003	8	ENABLED	DOWN	0 2
4	Dynamic	40000004	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 linkagg static agg admin-state command (see page 8-8) for static aggregate groups and with the linkagg lacp agg admin-state command (see page 8-16) for dynamic aggregate groups.
Oper State	The current operational state of the aggregate group, which can be UP or DOWN .
Att Ports	The number of ports actually attached to this aggregate group.
Sel Ports	The number of ports that could possibly attach to the aggregate group.

A static aggregate is specified:

```
-> show linkagg agg 5
```

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

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this static aggregate group.
Aggregate Number	The group number.
SNMP Descriptor	The standard MIB name for this static aggregate group.
Name	The name of this static aggregate group. You can modify this parameter with the linkagg static agg name command (see page 8-6).
Admin State	The administrative state of this static aggregate group, which can be ENABLED or DISABLED . You can modify this parameter with the linkagg static agg admin-state command (see page 8-8).
Operational State	The operational state of this static aggregate group, which can be UP or DOWN .
Aggregate Size	The number of links configured for this static aggregate group.
Number of Selected Ports	The number of ports that could possibly attach to this static aggregate group.
Number of Reserved Ports	The total number of ports reserved for use in link aggregation by this static aggregate group. (Note: This field is not relevant for static aggregate groups.)

output definitions (continued)

Number of Attached Ports	The number of ports actually attached to this static aggregate group.
Primary Port	The port number of the first port to join this static aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.

A dynamic aggregate group is specified:

```
-> show linkagg agg 1-2
```

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

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this dynamic aggregate group.
Aggregate Number	The group number of this dynamic aggregate group.
SNMP Descriptor	The standard MIB name for this dynamic aggregate group.
Name	The name of this dynamic aggregate group. You can modify this parameter with the linkagg lacp agg name command (see page 8-14).
Admin State	The administrative state of this dynamic aggregate group, which can be ENABLED or DISABLED . You can modify this parameter with the linkagg lacp agg admin-state command (see page 8-16).
Operational State	The operational state of this dynamic aggregate group, which can be UP or DOWN .
Aggregate Size	The number of links configured for this dynamic aggregate group.
Number of Selected Ports	The number of ports available to this dynamic aggregate group.
Number of Reserved Ports	The total number of ports reserved for use in link aggregation by this dynamic aggregate group.
Number of Attached Ports	The number of ports actually attached to this dynamic aggregate group.

output definitions (continued)

Primary Port	The port number of the first port to join this dynamic aggregate group. If the first port to join the aggregate group is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.
MACAddress	The MAC address associated with the primary port.
Actor System Id	The MAC address of this dynamic aggregate group. You can modify this parameter with the linkagg lacp agg actor system-id command (see page 8-21).
Actor System Priority	The priority of this dynamic aggregate group. You can modify this parameter with the linkagg lacp agg actor system-priority command (see page 8-19).
Actor Admin Key	The administrative key associated with this dynamic aggregate group. You can modify this parameter with the linkagg lacp agg actor admin-key command (see page 8-18).
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 linkagg lacp agg partner system-id command (see page 8-23).
Partner System Priority	The priority of the remote system to which this dynamic aggregation group is attached. You can modify this parameter with the linkagg lacp agg partner system-priority command (see page 8-25).
Partner Admin Key	The administrative key for the remote partner of the dynamic aggregation. You can modify this parameter with the linkagg lacp agg partner admin-key command (see page 8-27).
Partner Oper Key	The operational key of the remote system to which the dynamic aggregation group is attached.

Release History

Release 7.1.1; command introduced.

Related Commands

linkagg static agg size	Creates a static aggregate group.
linkagg lacp agg 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
  alclnkAggLocalRangeOperMin
  alclnkAggLocalRangeOperMax
  alclnkAggLocalRangeConfiguredMin
  alclnkAggLocalRangeConfiguredMax
  alclnkAggPeerRangeOperMin
  alclnkAggPeerRangeOperMax
  alclnkaggAggPartnerSystemID
  alclnkaggAggPartnerSystemPriority
  alclnkaggAggPartnerOperKey
```

show linkagg port

Displays information about link aggregation ports.

```
show linkagg {agg agg_num1 [-agg_num2]} port [slot/port]
```

Syntax Definitions

<i>agg_num1</i>	The number corresponding to the link aggregate group.
<i>-agg_num2</i>	The last link aggregate ID in a range of link aggregate IDs.
<i>slot</i>	The slot number for this aggregate.
<i>port</i>	The port number for this aggregate.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If no slot/port is specified, the information for all slots/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 a dynamic (LACP) aggregate group.
- If only a link aggregate or a range of link aggregates are specified along with the **agg** keyword, the port and related information for only the specified link aggregate IDs are displayed.
- If multi-chassis feature is activated on the switch, the show command displays the link aggregates as MC-Static and MC-Dynamic as shown in the second example.

Examples

```
-> show linkagg port
```

```
Slot/Port Aggregate  SNMP Id   Status   Agg  Oper Link Prim
-----+-----+-----+-----+-----+-----+-----+-----
  2/1   Static           2001  ATTACHED    1  UP   UP   YES
```

Multi-chassis active:

```
-> show linkagg port
```

```
Slot/Port Aggregate  SNMP Id   Status   Agg  Oper Link Prim
-----+-----+-----+-----+-----+-----+-----+-----
  2/1   MC-Static           2001  ATTACHED    1  UP   UP   YES
```

```
-> show linkagg agg 1-5 port
Slot/Port  Aggregate  SNMP Id    Status      Agg Oper Link Prim
-----+-----+-----+-----+-----+-----+-----+-----
  1/16  Static      2016      CONFIGURED    1   UP   UP   YES
  1/17  Static      2017      CONFIGURED    2   UP   UP   NO
  3/1   Static      3001      CONFIGURED    3   UP   UP   NO
  3/2   Static      3045      CONFIGURED    4   UP   UP   NO
  3/3   Static      3069      CONFIGURED    5   UP   UP   NO
```

Output fields are defined here:

output definitions

Slot/Port	The slot/port associated with the aggregate group.
Aggregate	The type of aggregate group associated with the port, either Static or Dynamic .
SNMP Id	The SNMP ID associated with the aggregate group.
Status	The current status of the port, which can be CONFIGURED , PENDING , SELECTED , or RESERVED .
Agg	The number of the aggregate groups associated with this port.
Oper	The operational status of the port.
Link	The physical link status of the port.
Prim	Specifies if the port is the primary port of the aggregate. The primary port is the lowest numbered port in a link aggregate.

A port that belongs to a static aggregate is specified:

```
-> show linkagg port 4/1
```

```
Static Aggregable Port
SNMP Id           : 4001,
Slot/Port         : 4/1,
Administrative State : ENABLED,
Operational State : DOWN,
Port State        : CONFIGURED,
Link State        : DOWN,
Selected Agg Number : 2,
Port position in the aggregate: 0,
Primary port      : NONE
```

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this port.
Slot/Port	The slot and port number.
Administrative State	The current administrative state of this port, which can be ENABLED or DISABLED .
Operational State	The current operational state of the port, which can be UP or DOWN .
Port State	The current operational state of the port, which can be CONFIGURED , PENDING , SELECTED , or RESERVED .

output definitions (continued)

Link State	The current operational state of the link from this port to its remote partner, which can be UP or DOWN .
Selected Agg Number	The number associated with the static aggregate group to which the port is attached.
Port position in the aggregate	The rank of this port within the static aggregate group.
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 static link aggregate is specified:

```
-> show linkagg agg 1
```

```
Static Aggregate
SNMP Id           : 40000001,
Aggregate Number  : 1,
SNMP Descriptor   : Omnichannel Aggregate Number 1 ref 40000001 size 4,
Name              : ,
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
```

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.aggl.syn0.col0.dis0.def1.exp0
Actor Oper State       : act1.tim1.aggl.syn0.col0.dis0.def1.exp0,
Partner Admin State    : act0.tim0.aggl.syn1.col1.dis1.def1.exp0,
Partner Oper State     : act0.tim0.aggl.syn0.col1.dis1.def1.exp0

```

Output fields are defined here:

output definitions

SNMP Id	The SNMP ID associated with this port.
Slot/Port	The slot and port number.
Administrative State	The current administrative state of this port, which can be ENABLED or DISABLED .
Operational State	The current operational state of the port, which can be UP or DOWN .
Port State	The current operational state of the port, which can be CONFIGURED , PENDING , SELECTED , or AGGREGATED .
Link State	The current operational state of the link from this port to its remote partner, which can be UP or DOWN .
Selected Agg Number	The number associated with the dynamic aggregate group to which the port is attached.
Primary Port	The port number of the first port to join this dynamic aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.
Actor System Priority	The actor system priority of this port. You can modify this parameter with the linkagg lacp port actor system-priority command (see page 8-36).
Actor System Id	The actor system ID (i.e., MAC address) of this port. You can modify this parameter with the linkagg lacp port actor system-id command (see page 8-34).
Actor Admin Key	The actor administrative key value for this port. You can modify this parameter with the linkagg lacp port actor admin-key command (see page 8-29).
Actor Oper Key	The actor operational key associated with this port.
Partner Admin System Priority	The administrative priority of the remote system to which this port is attached. You can modify this parameter with the linkagg lacp port partner admin system-priority command (see page 8-44).
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 system ID of a remote partner. This value is used along with Partner Admin System Priority, Partner Admin Key, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the linkagg lacp port partner admin system-id command (see page 8-40).

output definitions (continued)

Partner Oper System Id	The MAC address that corresponds to the system ID of the remote partner.
Partner Admin Key	The administrative value of the key for the remote partner. This value is used along with Partner Admin System Priority, Partner Admin System, Partner Admin Port, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the linkagg lacp port partner admin-key command (see page 8-42).
Partner Oper Key	The current operational value of the key for the protocol partner.
Attached Agg ID	The ID of the aggregate group that the port has attached itself to. A value of zero indicates that the port is not attached to an aggregate group.
Actor Port	The port number locally assigned to this port.
Actor Port Priority	The actor priority value assigned to the port. You can modify this parameter with the linkagg lacp port actor port priority command (see page 8-46).
Partner Admin Port	The administrative value of the port number for the protocol partner. This value is used along with Partner Admin System Priority, Partner Admin System ID, Partner Admin Key, and Partner Admin Port Priority to manually configure aggregation. You can modify this parameter with the linkagg lacp port partner admin-port command (see page 8-48).
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 manually configure aggregation. You can modify this parameter with the linkagg lacp port partner admin port-priority command (see page 8-50).
Partner Oper Port Priority	The priority value assigned to the this port by the partner.
Actor Admin State	The administrative state of the port. You can modify this parameter with the linkagg lacp port actor admin-state command (see page 8-32).
Actor Oper State	The current operational state of the port.
Partner Admin State	The administrative state of the partner port. You can modify this parameter with the linkagg lacp agg partner admin-state command (see page 8-38).
Partner Oper State	The current operational state of the partner port.

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

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

show linkagg range

Displays information about the configured or operational link aggregate range identifiers for standard and MC-LAG link aggregates.

show linkagg range [operation | config]

Syntax Definitions

operation Displays the operational ranges.

config Displays the configured ranges.

Defaults

By default, both the operational and configured ranges are shown.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **operation** parameter to display only the operational link aggregate identifiers.
- Use the **config** parameter to display only the configured link aggregate identifiers.
- A chassis reboot is required for the configured values to become operational.

Examples

```
-> show linkagg range
```

	Operational		Configured	
	Min	Max	Min	Max
Local	0	127	0	0
Peer	0	127	0	0
Multi-Chassis	0	127	0	127

output definitions

Operational Min/Max	The currently operational ranges.
Configured Min/Max	The currently configured ranges.
Local	The local link aggregate identifiers.
Peer	The peer link aggregate identifiers.
Multi-Chassis	The MC-LAG link aggregate identifiers.

Release History

Release 7.1.1; command introduced.

Related Commands

[linkagg range](#)

Configures the standard and MC-LAG aggregate identifier ranges.

MIB Objects

```
alclnkaggAggConfig
  alclnkAggLocalRangeOperMin
  alclnkAggLocalRangeOperMax
  alclnkAggLocalRangeConfiguredMin
  alclnkAggLocalRangeConfiguredMax
  alclnkAggPeerRangeOperMin
  alclnkAggPeerRangeOperMax
  alclnkAggPeerRangeConfiguredMin
  alclnkAggPeerRangeConfiguredMax
  alclnkAggMcLagRangeOperMin
  alclnkAggMcLagRangeOperMax
  alclnkAggMcLagRangeConfiguredMin
  alclnkAggMcLagRangeConfiguredMax
```

9 Multi-Chassis Commands

Multi-Chassis Link Aggregation (MC-LAG) enables dual homing of any standards based edge switches to two or more aggregation switches without running the Spanning Tree protocols between the edge and aggregation devices. The feature operates in a mode whereby all ports that are members of the multi-chassis aggregates are actively forwarding traffic. The overall system provides fast fail-over with a bound convergence time for all cases when edge uplinks fail.

MIB information for the Multi-Chassis commands is as follows:

Filename: ALCATEL-IND1-MULTI-CHASSIS-MIB.mib
Module: alcatelIND1MultiChassisMIB

A summary of available commands is listed here:

multi-chassis chassis-id
multi-chassis hello-interval
multi-chassis ipc-vlan
multi-chassis chassis-group
multi-chassis loop-detection
multi-chassis loop-detection transmit-interval
multi-chassis vf-link create
multi-chassis vf-link member-port
multi-chassis vf-link default-vlan
multi-chassis vip-vlan
show multi-chassis status
show multi-chassis loop-detection
show multi-chassis vf-link
show multi-chassis vf-link member-port
show multi-chassis consistency
show multi-chassis consistency linkagg
clear multi-chassis loop-detection

multi-chassis chassis-id

Assigns a globally unique chassis identifier to the switch and enables the switch to operate in multi-chassis mode.

multi-chassis chassis-id *chassis_id*

no multi-chassis chassis-id

Syntax Definitions

chassis_id Chassis ID number (1 or 2). The chassis ID must be unique within the set of switches configured to operate together providing multi-chassis services.

Defaults

parameter	default
<i>chassis_id</i>	0 (standalone mode; no multi-chassis operation is allowed)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to change the chassis ID back to “0” (the default). When the chassis ID is set to “0”, the switch operates in standalone mode and all multi-chassis related configuration commands are no longer active for the switch.
- Two switches that have the same chassis identifier are not allowed to operate in multi-chassis mode. If a duplicate chassis identifier is configured, the multi-chassis functionality will remain in a “down” operational state.
- A switch reboot is required for the configured chassis ID parameter value to become operational. In other words, any change to the chassis ID value is not implemented until the next switch reboot.
- MLAG is only supported between two peer switches of the same type and when both switches are running the same version of AOS Release 7. For example, MLAG is not supported between an OmniSwitch 10K and an OmniSwitch 6900 or between an OmniSwitch 6900 running 7.2.1.R01 and an OmniSwitch 6900 running 7.2.1.R02.

Examples

```
-> multi-chassis chassis-id 1
-> no multi-chassis chassis-id 1
```

Release History

Release 7.1.1; command introduced.

Related Commands

- show multi-chassis status** Displays the configured and operational parameters related to the multi-chassis feature on the switch.
- show multi-chassis consistency** Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```
multiChassisConfig  
  multiChassisConfigChassisId
```

multi-chassis hello-interval

Configures the multi-chassis hello interval parameter on the switch. Hello packets are sent periodically on the virtual fabric link (VFL) interfaces to establish a relationship and bidirectional communication between multi-chassis peer switches. The hello interval value determines how often these packets are sent.

multi-chassis hello-interval *seconds*

Syntax Definitions

seconds The number of seconds the switch waits between each transmission of a hello packet on the VFL. The valid range is 1–10 seconds.

Defaults

parameter	default
<i>seconds</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- The hello interval is a mandatory consistency parameter between two multi-chassis peer switches. The MCLAG protocol will not come up between the peer switches if each switch is configured with a different hello interval value.
- A switch reboot is required for the configured hello interval parameter value to become operational. In other words, any change to the hello interval value is not implemented until the next switch reboot.

Examples

```
-> multi-chassis hello-interval 2
```

Release History

Release 7.1.1; command introduced.

Related Commands

- multi-chassis chassis-id** Assigns a unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
- multi-chassis ipc-vlan** Configures the IPC-VLAN parameter, which is used for multi-chassis control communication, on the local switch.
- show multi-chassis status** Displays the configured and operational parameters related to the multi-chassis feature on the switch.
- show multi-chassis consistency** Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```
multiChassisConfig  
  multiChassisConfigHelloInterval
```

multi-chassis ipc-vlan

Configures a multi-chassis control VLAN, which is a special type of VLAN used to service inter-chassis communication between two multi-chassis peer switches.

multi-chassis ipc-vlan *vlan_id*

Syntax Definitions

vlan_id A VLAN ID number. The valid range is 2 - 4094 (VLAN 1 is not configurable as a multi-chassis control VLAN).

Defaults

parameter	default
<i>vlan_id</i>	4094

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines.

- This command is only supported on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Specify a VLAN ID that does not exist in the switch configuration. This command will automatically create the VLAN as a multi-chassis control VLAN.
- The control VLAN is a mandatory consistency parameter between two multi-chassis peer switches. The MLAG protocol will not come up between the peer switches if each switch is configured with a different control VLAN ID.
- A switch reboot is required for the configured control VLAN ID parameter value to become operational. In other words, any change to the control VLAN ID value is not implemented until the next switch reboot.
- Control VLANs are configured as a special VLAN type that is used only by MLAG. Assigning switch ports to a control VLAN, disabling the VLAN, or configuring Spanning Tree for the VLAN is not allowed.

Examples

```
-> multi-chassis ipc-vlan 100
```

Release History

Release 7.1.1; command introduced.

Related Commands

- multi-chassis chassis-id** Assigns a globally unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
- multi-chassis hello-interval** Configures the multi-chassis hello interval parameter on the switch.
- show multi-chassis status** Displays the configured and operational parameters related to the multi-chassis feature on the switch.
- show multi-chassis consistency** Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

multiChassisConfig
multiChassisConfigIpcVlan

multi-chassis chassis-group

Assigns a globally unique chassis group identifier to a multi-chassis peer switch. Each switch in a multi-chassis group (both peer switches) must use the same group ID number. The group ID number uniquely identifies a pair of switches operating in the multi-chassis mode.

multi-chassis chassis-group *group_id*

no multi-chassis chassis-group

Syntax Definitions

group_id Chassis group identifier. The valid range is 0–255.

Defaults

parameter	default
<i>group_id</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Use the **no** form of this command to set the chassis group ID to zero (the default).
- Each pair of multi-chassis peer switches must use a different group ID number to differentiate the group within the network environment.
- The group ID is appended to the MAC address generated for all MCLAG virtual IP (VIP) VLANs on a chassis to prevent duplicate MAC addresses from occurring in an MCLAG network environment. This is particularly important in a back-to-back MCLAG setup. However, configuring the group ID is recommended in all MCLAG configurations.
- It is not necessary to reboot the switch after configuring the group ID.
- The group ID number is a mandatory consistency parameter between two multi-chassis peer switches. The MCLAG protocol will not come up between the peer switches if each switch is configured with a different group ID number.
- There is no automatic detection or correction if two different multi-chassis domains are configured with the same group ID. Make sure each domain within the network uses a group ID number that is only associated with that domain.

Examples

```
-> multi-chassis chassis-group 10
-> no multi-chassis chassis-group
```

Release History

Release 7.2.1.R02; command introduced.

Related Commands

- | | |
|--|--|
| multi-chassis chassis-id | Assigns a unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode. |
| show multi-chassis status | Displays the configured and operational parameters related to the multi-chassis feature on the switch. |
| show multi-chassis consistency | Displays the system level mandatory consistency parameters of both the local and peer switches. |

MIB Objects

```
multiChassisConfig  
  multiChassisConfigChassisGroup
```

multi-chassis loop-detection

Configures the multi-chassis loop detection function for the switch. When a loop is detected, the ports that represent the point at which the loop was actually detected are automatically disabled.

multi-chassis loop-detection {enable | disable}

Syntax Definitions

enable	Enables loop detection.
disable	Disables loop detection.

Defaults

Loop detection is enabled by default on switches that operate in multi-chassis mode (the switch is configured with a multi-chassis ID of 1 or 2). The feature is disabled by default on switches that operate in standalone mode (no chassis ID is configured for the switch).

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Disabling loop detection is not recommended when configuring MCLAG in an existing network.
- Proprietary MAC addresses are used as the source addresses for loop detection control packets. Some of the OmniSwitch platforms are aware of these addresses will not learn them. However, other vendor switches will typically learn these addresses at the rate of one MAC address per VLAN.

Examples

```
-> multi-chassis loop-detection enable
-> multi-chassis loop-detection disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

multi-chassis loop-detection transmit-interval

Configures the amount of time the switch waits between each transmission of successive Loop Detection packets on each active VLAN.

show multi-chassis loop- detection

.Displays the loop detection status and parameter values for the switch.

clear multi-chassis loop- detection

Clears the MC-LAG loop detection information maintained by the switch.

MIB Objects

```
multiChassisConfig  
  multiChassisConfigLoopDetectionAdminStatus
```

multi-chassis loop-detection transmit-interval

Configures the loop detection transmit interval parameter. When loop detection is enabled, the switch generates multicast loop detection PDU (LDPDU) on each active VLAN. The loop detection transmit interval determines how often the LDPDU are sent.

multi-chassis loop-detection transmit-interval *seconds*

Syntax Definitions

seconds The number of seconds the switch waits between each transmission of a loop detection packets. The valid range is 1–10 seconds.

Defaults

parameter	default
<i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Increasing the transmit interval time as the number of configured VLANs increases is recommended to minimize the amount of bandwidth consumed by loop detection control packets. For example, if thousands of VLANs are configured on the switch, set the transmit interval to a number close or equal to ten seconds instead of using the default value of one second.

Examples

```
-> multi-chassis loop-detection transmit-interval 2
-> multi-chassis loop-detection transmit-interval 3
```

Release History

Release 7.1.1; command introduced.

Related Commands

- multi-chassis loop-detection** Configures the multi-chassis loop detection function on the switch.
- show multi-chassis loop-detection** Displays the loop detection status and parameter values for the switch.

MIB Objects

```
multiChassisConfig  
  multiChassisLoopDetectionTransmitInterval
```

multi-chassis vf-link create

Configures a virtual fabric link (VFL) between two peer switches. A VFL is required to enable the MCLAG operation between the two switches.

multi-chassis vf-link create

no multi-chassis vf-link

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Use the **no** form of this command to remove the VFL configuration from the switch.
- Although the switch supports runtime configuration of the VFL and its member ports, configuring the VFL at the same time as the chassis ID is configured and before rebooting the switch is recommended.

Examples

```
-> multi-chassis vf-link create
-> no multi-chassis vf-link
```

Release History

Release 7.1.1; command introduced.

Related Commands

multi-chassis vf-link member-port	Configures the member port list for the virtual fabric link.
multi-chassis vf-link default-vlan	Configures the default VLAN on the virtual fabric link.
show multi-chassis vf-link	Displays information about the virtual fabric link on the switch.
show multi-chassis vf-link member-port	Displays detailed information about the virtual fabric link member ports on the switch.

MIB Objects

```
multiChassisLinkTable  
  multiChassisLinkIfIndex  
  multiChassisLinkOperStatus  
  multiChassisLinkActivePortNum  
  multiChassisLinkRowStatus
```

multi-chassis vf-link member-port

Configures member ports for the virtual fabric link (VFL).

multi-chassis vf-link member-port *slot/port*

no multi-chassis vf-link member-port *slot/port*

Syntax Definitions

slot/port

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 10K, 6900

Usage Guidelines

- This command is only available on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- The maximum number of ports that can be configured as virtual fabric link members is 8.
- Currently, only ports capable of operating at 10 Gbps (XNI-U32 only on OmniSwitch 10K) and in full duplex mode can support the virtual fabric link operation. Ports on other types of modules are not eligible to become virtual fabric link member ports.
- If an eligible port is operationally down when the port is configured as a member of the VFL, the configuration is accepted. When that port then becomes operational, however, the switch will verify the port is operating at the required speed and duplex mode before accepting the port as a member. If these conditions are not met, the VFL configuration is removed from the port and a syslog message and SNMP trap are generated.
- Although the switch supports runtime configuration of the VFL and its member ports, configuring the VFL at the same time as the chassis ID is configured and before rebooting the switch is recommended.
- The virtual fabric link member ports become operational only when the switch comes up running in the multi-chassis mode. In other words, runtime configuration of a chassis identifier on a switch currently operating in standalone mode does not activate the member ports.
- For resiliency reasons, configuring at least 4 ports as virtual fabric link members is recommended. An ideal set up would be to have two ports configured per network interface card. Within each network interface card, using a port in the lower range of port numbers (1 through 16) and one port in the higher range of port numbers (17 through 32) is recommended.

Examples

```
-> multi-chassis vf-link member-port 3/1
-> no multi-chassis vf-link member-port 3/2
```

Release History

Release 7.1.1; command introduced.

Related Commands

multi-chassis vf-link create	Configures a virtual fabric link between two peer switches to enable them to operate in multi-chassis mode.
multi-chassis vf-link default-vlan	Configures the default VLAN on the virtual fabric link.
show multi-chassis vf-link	Displays information about the virtual fabric link on the switch.
show multi-chassis vf-link member-port	Displays detailed information about the virtual fabric link member ports on the switch.

MIB Objects

```
multiChassisLinkMemberPortTable  
  multiChassisLinkMemberPortLinkIfIndex  
  multiChassisLinkMemberPortIfindex  
  multiChassisLinkMemberPortOperStatus  
  multiChassisLinkMemberPortRowStatus
```

multi-chassis vf-link default-vlan

Configures the default VLAN for the virtual fabric link (VFL).

multi-chassis vf-link default-vlan *vlan_id*

no multi-chassis vf-link default-vlan

Syntax Definitions

vlan_id An existing VLAN ID number to assign as the default VLAN for the VFL. The valid range is 1–4094.

Defaults

parameter	default
<i>vlan_id</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is only supported on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Use the **no** form of this command to remove the default VLAN assignment from the VFL.
- When no configuration is explicitly provided, the default or untagged VLAN for the virtual fabric link is VLAN 1.
- Specify a VLAN ID that already exists in the switch configuration.
- If the VLAN currently configured as the default VLAN for the virtual fabric link is removed using VLAN management commands (**no vlan** *vlan_id*), VLAN 1 is automatically reinstated as the default VLAN for the virtual fabric link.

Examples

```
-> vlan 2 admin-state enable
-> multi-chassis vf-link default-vlan 2
-> no multi-chassis vf-link default-vlan
-> no vlan 2
```

Release History

Release 7.1.1; command introduced.

Related Commands

multi-chassis vf-link create	Configures a virtual fabric link between two peer switches to enable them to operate in multi-chassis mode.
show multi-chassis vf-link member-port	Configures the member port list for the virtual fabric link.
show multi-chassis vf-link	Displays information about the virtual fabric link on the switch.
show multi-chassis vf-link member-port	Displays detailed information about the virtual fabric link member ports on the switch.

MIB Objects

```
multiChassisLinkTable  
  multiChassisLinkfIndex  
  multiChassisLinkMemberPortLinkIfIndex,  
  multiChassisLinkMemberPortOperDefaultVlan
```

multi-chassis vip-vlan

Configures a virtual IP (VIP) VLAN, which is a special type of VLAN used to provide the underlying LAN infrastructure for the support of basic IP/Layer 3 services on a multi-chassis link aggregation group.

multi-chassis vip-vlan *vlan_id[-vlan_id2]*

no multi-chassis vip-vlan *vlan_id[-vlan_id2]*

Syntax Definitions

vlan_id[-vlan_id2]

VLAN ID number (2–4093). Use a hyphen to specify a range of VLAN ID numbers (200-210).

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is only supported on switches that are configured with a valid multi-chassis chassis ID number (1 or 2).
- Use the **no** form of this command to remove a VIP VLAN from the switch configuration.
- Specify a VLAN ID that does not exist in the switch configuration. This command will automatically create the VLAN as a VIP VLAN.
- Although VIP VLANs are identified as a special VLAN type for MCLAG purposes, assigning non-MCLAG ports to this type of VLAN is supported. In addition, assigning MCLAG ports to standard VLANs (non-VIP VLANs) is supported.
- The IP interfaces configured on a VIP VLAN cannot be bound to any routing protocols or establish routing adjacencies
- VRRP is not supported on VIP VLAN IP interfaces.
- IPv6 interfaces cannot be configured on a virtual IP VLAN at this time.
- There are two IP addresses associated with a VIP VLAN IP interface: a management address and a virtual IP address.
 - The management address is a unique IP address used by each switch within a multi-chassis domain to provide management services. Each peer switch must have a unique management IP address.
 - The virtual IP address is used to route packets that terminate on the multi-chassis peer switches. Unlike the management address, the VIP address must be the same on each peer switch.

Examples

```
-> multi-chassis vip-vlan 3
-> multi-chassis vip-vlan 10-15
-> no multi-chassis vip-vlan 3
-> no multi-chassis vip-vlan 10-15
```

Release History

Release 7.1.1; command introduced.

Release 7.2.1.R02; restriction as to the type of ports assigned to VIP VLANs was removed. In addition, MCLAG ports can now also be assigned to standard VLANs.

Related Commands

multi-chassis chassis-id	Assigns a unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
ip interface	Configures an IP interface for a VLAN. Use this command to configure an IPv4 interface for a VIP VLAN.
show vlan	Displays the list of VLANs configured for the switch. Includes VLAN type, such as VIP VLAN.

MIB Objects

```
vlanTable
  vlanEntry
```

show multi-chassis status

Displays the configured and operational parameters related to the multi-chassis feature on the switch.

show multi-chassis status

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

NA

Examples

```
-> show multi-chassis status
Multi-Chassis      Operational      Configured
-----+-----+-----
Chassis ID         1                2
Chassis Role       Primary          N/A
Status             UP              N/A
Chassis-Type       OS10K           N/A
Hello Interval     1s              1s
IPC VLAN           4904            4094
Chassis-Group      10              10
```

Output fields are defined here:

output definitions

Operational	Operational parameters are the parameters that are currently being used by the system.
Configured	Often time, within the scope of the multi-chassis feature, the term " configured " is commonly used to identify parameters that have been configured, but that will be implemented after the next switch reset.
Chassis ID	Chassis identifier within the multi-chassis operational range [1 - 2]. The chassis identifier must be globally unique within the set of switches configured to operate together providing multi-chassis services.
Chassis Role	The chassis role determines which of the switches operating in multi-chassis mode is the master of the combined system. The role information can be used by various software components as needed.
Status	The current status of the multi-chassis feature, which can be Down , Up , or Inconsistent .

output definitions

Chassis-Type	The peer switch chassis type (OS6900 or OS10K).
Hello Interval	Time interval, in seconds, at which multi-chassis control hello messages are to be sent to the peer switch within the range [1 - 10].
IPC VLAN	Multi-chassis control VLAN used for all multi-chassis control communication between the peer switches within the range [2 - 4094].
Chassis-Group	The multi-chassis group ID for the switch. Both peer switches must use the same group ID.

Release History

Release 7.1.1; command introduced.

Release 7.2.1; **Chassis-Type** and **Chassis-Group** fields added.

Related Commands

multi-chassis chassis-id	Assigns a globally unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
multi-chassis hello-interval	Configures the multi-chassis hello interval parameter on the switch.
multi-chassis ipc-vlan	Configures the IPC-VLAN parameter, which is used for multi-chassis control communication, on the local switch.
show multi-chassis consistency	Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

```

multiChassisOperation
  multiChassisOperChassisId
  multiChassisOperChassisRole
  multiChassisOperStatus
  multiChassisOperHelloInterval
  multiChassisOperIpcVlan
multiChassisConfig
  multiChassisConfigChassisId
  multiChassisConfigHelloInterval
  multiChassisConfigIpcVlan

```

show multi-chassis loop-detection

Displays the configured and operational parameters related to the multi-chassis loop-detection feature on the switch.

show multi-chassis loop-detection

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If a loop is detected, disable loop detection then use **clear multi-chassis loop-detection** command to clear the loop detection information from the ports that were downed. This will ensure that **show multi-chassis loop-detection** command displays the most current status for such ports.

Examples

```
-> show multi-chassis loop-detection
Status                : Enabled,
Transmit Interval     : 1s,
Total Transmit Count  : 1256,
Total Loop Count      : 10,
Port Down List        : 2/4 1/3 5/6
```

output definitions

Status	Administrative status of the loop-detection feature, which can be Enabled or Disabled
Transmit Interval	Transmit interval, in seconds, which determines the time interval between the transmission of successive loop-detection packets on each VLAN active on the switch within the range [1 - 10].
Total Transmit Count	Total number of control packets transmitted on all VLANs configured on the switch.
Total Loop Count	Total number of control packets that were transmitted and received, i.e. looped back to the originator on all VLANs.
Port Down List	List of ports that were brought down because a loop was detected.

Release History

Release 7.1.1; command introduced.

Related Commands

multi-chassis loop-detection	Configures the multi-chassis loop-detection function on the switch.
multi-chassis loop-detection transmit-interval	Configures the loop-detection transmit interval, which determines the time interval between the transmission of successive loop-detection packets on each VLAN active on the switch.
clear multi-chassis loop-detection	Clears the MC-LAG loop detection information maintained by the switch.

MIB Objects

```
multiChassisLoopDetection
  multiChassisLoopDetectionTransmitCount
  multiChassisLoopDetectionCount
  multiChassisLoopDetectionPortDownList
  multiChassisLoopDetectionAdminStatus
  multiChassisLoopDetectionTransmitInterval
```

show multi-chassis vf-link

Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

show multi-chassis vf-link

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

NA

Examples

```
-> show multi-chassis vf-link
VFLink ID  Oper      Primary Port  Config Port  Active Port  Def Vlan
-----+-----+-----+-----+-----+-----
0          Up        1/2          4            4            5
```

output definitions

VFLink ID	Virtual Fabric Link identifier. Currently a single virtual fabric link with identifier equal to zero is supported.
Oper	The current status of the Virtual Fabric Link, which can be Disabled , Down or Up . The Disabled state occurs whenever the multi-chassis feature is disabled because the operational chassis identifier currently effective is the standalone chassis identifier, i.e. zero.
Primary Port	Identifies the primary port of the virtual fabric link. This concept is relevant because all the non-unicast traffic (i.e. broadcast, multicast and unknown unicast) is distributed across ports of the network interface module that hosts the virtual fabric link's primary port.
Config Port	Number of physical ports configured as virtual fabric link member ports in the range [0 - 8].
Active Port	Number of physical ports that are operational or active members of the virtual fabric link in the range [0 - 8].
Def Vlan	Default VLAN on the virtual fabric link within the range [1 - 4094].

Release History

Release 7.1.1; command introduced.

Related Commands

- | | |
|---|--|
| multi-chassis vf-link create | Configures a virtual fabric link between two peer switches to enable them to operate in multi-chassis mode. |
| multi-chassis vf-link member-port | Adds a port to the list of member ports of the virtual fabric link. |
| multi-chassis vf-link default-vlan | Configures the default VLAN on the virtual fabric link. |
| show multi-chassis vf-link member-port | Displays detailed information about the configured and operational parameters related to the virtual fabric link member ports on the switch. |

MIB Objects

```
multiChassisLinkTable
  multiChassisLinkIfIndex
  multiChassisLinkOperStatus
  multiChassisLinkPrimaryPort
  multiChassisLinkConfigPortNum
  multiChassisLinkActivePortNum
vlanTable
  vlanEntry
```

show multi-chassis vf-link member-port

Displays detailed information about the configured and operational parameters related to the virtual fabric link member ports on the switch.

show multi-chassis vf-link member-port [*slot/port*]

Syntax Definitions

slot/port Specify the slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

NA

Examples

```
-> show multi-chassis vf-link member-port
VFLink ID  Slot/Port  Oper      Is Primary
-----+-----+-----+-----
0           1/1         Up        No
0           1/2         Up        Yes
0           1/17        Up        No
0           1/18        Up        No

-> show multi-chassis vf-link member-port 3/1
VFLink ID  Slot/Port  Oper      Is Primary
-----+-----+-----+-----
0           1/2         Up        Yes
```

output definitions

VFLink ID	Virtual fabric link identifier. Currently a single virtual fabric link with identifier equal to zero is supported.
Slot/Port	The slot/port that defines each of the physical ports that are members of the virtual fabric link.
Oper	The current status of each virtual fabric link member port, which can be Disabled , Down or Up . The Disabled state occurs whenever the multi-chassis feature is disabled because the chassis is operating in stand-alone mode.
Is Primary	Indicates whether or not (Yes or No) the virtual fabric link member port is the primary port for the link.

Release History

Release 7.1.1; command introduced.

Related Commands

multi-chassis vf-link create	Configures a virtual fabric link between two peer switches to enable them to operate in multi-chassis mode.
multi-chassis vf-link member-port	Adds a port to the list of member ports of the virtual fabric link.
multi-chassis vf-link default-vlan	Configures the default VLAN on the virtual fabric link.
show multi-chassis vf-link	Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

MIB Objects

```
multiChassisLinkMemberPortTable  
  multiChassisLinkMemberPortLinkIfIndex,  
  multiChassisLinkMemberPortIfIndex,  
  multiChassisLinkMemberPortOperStatus  
  multiChassisLinkMemberPortIsPrimary
```

show multi-chassis consistency

Displays the system level mandatory consistency parameters for both the local and peer switches.

show multi-chassis consistency

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

NA

Examples

```
-> show multi-chassis consistency
Consistency          Local      Peer      Status
-----+-----+-----+-----
Chassis-ID           1          2          OK
Chassis-Type         OS10K     OS10K     OK
Hello-Interval       1          1          OK
IPC-VLAN              4094      4094      OK
Chassis-Group        1          1          OK
STP-Path-Cost-Mode   Auto       Auto       OK
STP-Mode              Per-VLAN  Per-VLAN  OK
```

Output fields are defined here:

output definitions

Consistency	Provides a list of global mandatory consistency parameters for the local and remote switches operating in multi-chassis mode.
Local	Value of a given consistency parameter on the local switch.
Peer	Value of a given consistency parameter on the peer switch.
Status	Specifies the overall status of a consistency parameter within the entire multi-chassis system comprised by the individual switches. The possible values are OK , NOK or N/A . or If there is a mismatch of any of the parameters listed in this command or if the chassis identifier of the two switches is the same, the multi-chassis operational status will not become Up. In this case the "Status" column shown in this output will indicate which parameter has a problem. The N/A value in the "Peer" column indicates that the information is unavailable from the peer. This will always be the case when the multi-chassis operational status is Down .

output definitions

Chassis-ID	Globally unique chassis identifier. The valid range for the multi-chassis operational range is [1 - 2], whereas the value for standalone operation is zero.
Chassis-Type	The peer switch chassis type (OS6900 or OS10K).
Hello Interval	Time interval, in seconds, at which multi-chassis control hello messages are to be sent to the peer switch within the range [1 - 10].
IPC VLAN	Multi-chassis control VLAN used for all multi-chassis control communication between the peer switches within the range [2 - 4094].
Chassis-Group	The multi-chassis group ID for the switch. Both peer switches must use the same group ID.
STP-Path-Cost-Mode	Specifies the STP path cost mode whose possible values are Auto and 32Bit.
STP-Mode	Specifies the STP mode (Per-VLAN or Flat)

Release History

Release 7.1.1; command introduced.

Release 7.2.1:R02; **Chassis-Type** and **Chassis-Group** fields added.

Related Commands

spantree mode	Assigns a flat Spanning Tree or per-vlan Spanning Tree operating mode for the switch. These modes are exclusive; however, it is not necessary to reboot the switch when the STP modes are changed.
multi-chassis chassis-id	Assigns a globally unique chassis identifier to the switch and enables or disables the switch to operate in multi-chassis mode.
multi-chassis hello-interval	Configures the multi-chassis hello interval parameter on the switch.
multi-chassis ipc-vlan	Configures the IPC-VLAN parameter, which is used for multi-chassis control communication, on the local switch.
show multi-chassis status	Displays the configured and operational parameters related to the multi-chassis feature on the switch.
show multi-chassis consistency linkagg	Displays the per-multi-chassis aggregate level optional consistency parameters of both the local and peer switches.

MIB Objects

```

multiChassisGlobalConsistency
  multiChassisLocalChassisId
  multiChassisPeerLocalChassisId
  multiChassisIdConsistency
  multiChassisLocalChassisType
  multiChassisPeerChassisType
  multiChassisTypeConsistency
  multiChassisLocalHelloInterval
  multiChassisPeerHelloInterval
  multiChassisHelloIntervalConsistency
  multiChassisLocalIpcVlan
  multiChassisPeerIpcVlan
  multiChassisIpcVlanConsistency

```

```
multiChassisLocalChassisGroup  
multiChassisPeerChassisGroup  
multiChassisGroupConsistency  
multiChassisLocalStpPathCostMode  
multiChassisPeerStpPathCostMode  
multiChassisStpPathCostModeConsistency  
multiChassisLocalStpMode  
multiChassisPeerStpMode  
multiChassisStpModeConsistency
```

show multi-chassis consistency linkagg

Displays the per-multi-chassis aggregate level optional consistency parameters of both the local and peer switches.

show multi-chassis consistency linkagg [*agg_id* [**vlan-list**] | **vlan-list**]

Syntax Definitions

agg_id A multi-chassis link aggregate ID number. The valid range is 0–127.

vlan-list Lists the local and peer VLANs associated with the aggregate.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command provides data related to multi-chassis aggregates only. It cannot be used for ordinary aggregates. In order to determine the type of an aggregate and classify this aggregate as a multi-chassis aggregate the user must use the [linkagg range](#) command.
- The user must be aware of the ranges assigned to aggregate identifiers by using the [linkagg range](#) command.
- Mismatches of any of the parameters listed in this command represent network mis-configurations and may cause traffic problems. In this case the "Status" column shown in this output will indicate which parameter has a problem.

Examples

```
-> show multi-chassis consistency linkagg
```

```
      Local Peer
Linkagg Exist Exist Status
-----+-----+-----+-----
3 Yes    Yes    OK    OK
```

```
-> show multi-chassis consistency linkagg 3
```

```
Consistency          Local          Peer          Status
-----+-----+-----+-----
Chassis-ID           1             2             OK
Agg-ID                3             3             OK
LAG-Type              MC-LACP       MC-SATIC      NOK
LACP-System-ID        00:d0:95:a3:ec:67  00:d0:95:a3:ec:67  OK
LACP-Priority         100           100           OK
Default-Vlan          1             1             OK
VLAN List             Configured     Configured     NOK
```

```
-> show multi-chassis consistency linkagg 100 vlan-list
Agg-ID      : 100,
Local Count : 3,
Peer Count  : 3
```

Ref	Vlan	Type	Admin	Oper	IP	Mtu	Mac		Vpa-State	Vrf	ICMP	
							learn	Vpa-Type			redir	Status
Local	1	Std	Ena	Ena	Dis	1500	Ena	Default	Forward	0	Dis	OK
Peer	1	Std	Ena	Ena	Dis	1500	Ena	Default	Forward	0	Dis	OK
Local	100	Std	Ena	Ena	Dis	1500	Ena	Qtagged	Forward	0	Dis	OK
Peer	100	Std	Ena	Ena	Dis	1500	Ena	Qtagged	Forward	0	Dis	OK
Local	200	Vip	Ena	Ena	Dis	1500	Ena	Qtagged	Forward	0	Dis	OK
Peer	200	Vip	Ena	Ena	Dis	1500	Ena	Qtagged	Forward	0	Dis	OK

output definitions

Consistency	Provides a list of per-multi-chassis aggregate optional consistency parameters for the local and remote switches operating in multi-chassis mode.
Local/Peer Exist	Specifies if the Link Agg exists on both local and peer chassis.
Local/Peer	Value of a given consistency parameter on the local/peer switch.
Status	Specifies the overall status of a consistency parameter within the entire multi-chassis system comprised by the individual switches. The possible values are OK , NOK or N/A . or If there is a mismatch of any of the parameters listed in this command or if the chassis identifier of the two switches is the same, the multi-chassis operational status will not become Up. In this case the "Status" column shown in this output will indicate which parameter has a problem. The N/A value in the "Peer" column indicates that the information is unavailable from the peer. This will always be the case when the multi-chassis operational status is Down .
Chassis-ID	Globally unique chassis identifier. The valid range for the multi-chassis operational range is [1 - 2], whereas the value for standalone operation is zero.
Agg-ID	The number corresponding to the static or dynamic multi-chassis aggregate group within the range [0-127].
LAG-Type	Defines the aggregate type as static or dynamic, i.e. LACP
LACP-System-ID	Specifies the system identifier (MAC address format) used by the LACP protocol.
LACP-Priority	Provides the system priority used by the LACP protocol.
Default-Vlan	Specifies the value of the default VLAN configured on the multi-chassis aggregate within the range [1 - 4094].
VLAN List	Indicates whether other types of VLANs (distinct from the default VLAN) are configured on the multi-chassis aggregate.
Local/Peer Count	The number of VLANs on the local/peer chassis.

Release History

Release 7.1.1; command introduced.

Release 7.2.1; **vlan-list** parameter added.

Related Commands

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

MIB Objects

```
multiChassisLinkaggConsistencyTable
  multiChassisLinkaggAggIndex
  multiChassisLinkaggAggIndexConsistency
  multiChassisLinkaggLocalAggType
  multiChassisLinkaggPeerAggType
  multiChassisLinkaggAggTypeConsistency
  multiChassisLinkaggLocalVlanType
  multiChassisLinkaggPeerVlanType
  multiChassisLinkaggVlanTypeConsistency
  multiChassisLinkaggLocalVlanListConfig
  multiChassisLinkaggLocalVlanListConfigConsistency
  multiChassisLinkaggVlanListConfigConsistency
  multiChassisLinkaggLocalAggActorSystemID
  multiChassisLinkaggPeerAggActorSystemID
  multiChassisLinkaggAggActorSystemIDConsistency
  multiChassisLinkaggLocalAggActorSystemPriority
  multiChassisLinkaggPeerAggActorSystemPriority
  multiChassisLinkaggAggActorSystemPriorityConsistency
```

clear multi-chassis loop-detection

Clears the configured and operational parameters related to the multi-chassis loop-detection feature on the switch.

clear multi-chassis loop-detection

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If a loop is detected, disable loop detection then use **clear multi-chassis loop-detection** command to clear the loop detection information from the ports that were downed. This will ensure that **show multi-chassis loop-detection** command displays the most current status for such ports.

Examples

```
-> clear multi-chassis loop-detection
```

Release History

Release 7.1.1; command introduced.

Related Commands

multi-chassis loop-detection	Configures the multi-chassis loop-detection function on the switch.
show multi-chassis loop-detection	Displays the configured and operational parameters related to the multi-chassis loop-detection feature on the switch.

MIB Objects

multiChassisLoopDetection

10 Ethernet Ring Protection Commands

Ethernet Ring Protection (ERP) is a protection switching mechanism for Ethernet ring topologies, such as multi-ring and ladder networks. The implementation of ERP on Alcatel-Lucent OmniSwitch is based on ERP Version 2 (ITU-T G.8032/Y.1344 to 2010) using the Ring Automatic Protection Switching (R-APS) protocol to coordinate and prevent network loops within a bridged Ethernet ring.

ERPV2 supports multi-rings and ladder to ladder networks. ERPv2 functionalities allow configuration of Sub-Rings within a Master Ethernet Ring, interconnected nodes and shared links between the rings.

MIB information for Ethernet Ring Protection commands is as follows:

Filename: AlcatelIND1Erp.mib
Module: ALCATEL-IND1-ERP-MIB

A summary of available commands is listed here:

erp-ring
erp-ring rpl-node
erp-ring wait-to-restore
erp-ring enable
erp-ring guard-timer
erp-ring sub-ring
erp-ring virtual-channel
erp-ring revertive
erp-ring clear
erp-ring ethoam-event
clear erp statistics
show erp
show erp statistics
show erp statistics

erp-ring

Creates an Ethernet Ring Protection (ERP) using the specified ports and service VLAN ID. The service VLAN transmits ERP control traffic, such as Ring Automatic Protection Switching (R-APS) messages, through the ring. The specified level number identifies an APS Management Entity Group (MEG) to which the service VLAN belongs.

erp-ring *ring_id* **port1** {*slot/port* | **linkagg** *agg_num*} **port2** {*slot/port* | **linkagg** *agg_num*} **service-vlan** *vlan_id* **level** *level_num* [**guard-timer** *guard_timer*] [**wait-to-restore-timer** *wtr_timer*] [**enable** | **disable**]

no erp-ring *ring_id*

Syntax Definitions

<i>ring_id</i>	The ERP ring ID number. The valid range is 1 to 2147483647.
<i>slot/port</i>	The slot number for the module and the physical port number on that module.
<i>agg_num</i>	The link aggregate ID number.
<i>vlan_id</i>	The service VLAN ID number. The valid range is 1 to 4094.
<i>level_num</i>	The MEG level number for the service VLAN. The valid range is 0 to 7.
<i>guard-timer</i>	The guard timer value, in centi seconds, for the ring node.
<i>wtr-timer</i>	The wait-to-restore timer value, in minutes, for the Ring Protection Link (RPL) node.
enable	Administratively enables the ERP ring.
disable	Administratively disables the ERP ring.

Defaults

parameter	default
<i>guard_timer</i>	50
<i>wtr_timer</i>	5
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a ring from the switch configuration. Administratively disable the ring ports before deleting the ring to avoid creating any network loops. Once the ring is deleted, ensure that the same ports are administratively enabled under Spanning Tree control.
- The specified ring identification number must be unique within a switch.

- ERP is not supported on mobile ports, mirroring ports, link aggregate member ports, high availability ports, Multicast VLAN receiver ports (ERP is supported on Multicast VLAN sender ports only), VLAN Stacking user network interface (UNI) ports, or RRSTP ring ports.
- If a port is tagged with the service VLAN ID or the service VLAN is the default VLAN for the port, then the port is not eligible to become an ERP ring port.
- Specify an existing VLAN ID for the service VLAN ID. Use the same VLAN ID and level number for the service VLAN on each switch that participates in the ERP ring.
- If the ERP switch participates in an Ethernet OAM Maintenance Domain (MD), configure the ERP service VLAN to use the same level number that is used for the Ethernet OAM MD.
- Specify a static VLAN ID for the ERP service VLAN; dynamic VLANs are not configurable as service VLANs.
- The service VLAN can belong to only one ERP ring at a time. A maximum of 64 rings are allowed per switch.
- The specified service VLAN ID must not participate in a Spanning Tree instance that is associated with non-ERP VLANs. Ideally, change the Spanning Tree configuration for the VLAN ID prior to using this command.
- An ERP ring port can belong to only one ERP ring at a time.
- Create an ERP type NNI-SVLAN binding before establishing an ERP ring on that SVLAN-NNI binding.

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 7.1.1; command introduced.

Related Commands

show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.
ethernet-service svlan nni	Creates an NNI-SVLAN binding.

MIB Objects

alaErpRingTable

- alaErpRingServiceVid
- alaErpRingMEGLevel
- alaErpRingStatus
- alaErpRingPort1
- alaErpRingPort2
- alaErpRingWaitToRestore
- alaErpRingGuardTimer
- alaErpRingRowStatus

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

<i>ring_id</i>	An existing ERP ring ID number. The valid range is 1 to 2147483647.
<i>slot/port</i>	The slot number for the module and the physical port number on that module.
<i>agg_num</i>	The link aggregate ID number.

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

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 Ethernet ring while it is enabled is rejected.
- The specified ERP ring ID must exist in the switch configuration.
- This command applies only to ERP ring ports; ports not configured as ERP ring ports are not eligible to become RPL ports.
- Only one of the two ring ports configured for the switch can be designated as an RPL node port.

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 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
erp-ring wait-to-restore	Configures the wait-to-restore timer value for the Ring Protection Link (RPL) node.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingPortEntry  
  alaErpRingPortIfIndex  
  alaErpRingPortType
```

erp-ring wait-to-restore

Configures the wait-to-restore timer value for the 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

<i>ring_id</i>	An existing ERP ring ID number. The valid range is 1 to 2147483647.
<i>wtr_timer</i>	The number of minutes to wait before restoring the RPL to a blocked state. The valid range is 1 to 12.

Defaults

By default, the wait-to-restore timer value is set to 5 minutes.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to set the timer back to the default setting of 5 minutes.
- The specified ERP ring ID must exist in the switch configuration.
- This command applies only on a switch that serves as the RPL node for the ERP ring.

Examples

```
-> erp-ring 1 wait-to-restore 6  
-> no erp-ring 1 wait-to-restore
```

Release History

Release 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
erp-ring rpl-node	Configures a Ring Protection Link (RPL) port connection.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId  
  alaErpRingWaitToRestoreTimer
```

erp-ring enable

Enables or disables an ERP ring identified by the specified ring ID. This command applies to enabling or disabling existing ERP rings.

erp-ring *ring_id* {**enable** / **disable**}

Syntax Definitions

ring_id An existing ERP ring ID number. The valid range is 1to2147483647.

Defaults

By default, ERP rings are disabled when they are created.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The specified ring ID must exist in the switch configuration.
- Enabling a ring is also allowed at the time the ring is created.

Examples

```
-> erp-ring 1 enable
-> erp-ring 1 disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId
  alaErpRingStatus
```

erp-ring guard-timer

Configures the guard timer value for the specified ERP ring node. The guard timer is used to prevent ring nodes from receiving outdated Ring Automatic Protection Switching (R-APS) messages. During the amount of time determined by this timer, all received R-APS messages are ignored by the ring protection control process.

```
erp-ring ring_id guard-timer guard_timer
```

```
no erp-ring ring_id guard-timer
```

Syntax Definitions

ring_id An existing ERP ring ID number. The valid range is 1–2147483647.
guard_timer The guard timer value. The valid range is 1–200 centi-secs.

Defaults

parameter	default
<i>guard_timer</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to set the timer back to the default value of 50 centi-secs.
- The specified ring ID must exist in the switch configuration.

Examples

```
-> erp-ring 1 guard-timer 10  
-> no erp-ring 1 guard-timer
```

Release History

Release 7.1.1; command introduced.

Related Commands

[erp-ring](#) Configures an ERP ring.
[show erp](#) Displays the ERP ring configuration for the switch.

MIB Objects

```
alaErpRingId  
alaErpRingGuardTimer
```

erp-ring sub-ring

Creates an Ethernet Ring Protection (ERP) sub-ring.

```
erp-ring ring_id sub-ring-port {slot/port | linkagg agg_num} service-vlan vlan_id level level_num
[guard-timer guard_timer] [wait-to-restore-timer wtr_timer] [enable | disable]
```

Syntax Definitions

<i>ring_id</i>	The ERP ring ID number. The valid range is 1 to 2147483647.
<i>slot/port</i>	The slot number for the module and the physical port number on that module.
<i>agg_num</i>	The link aggregate ID number.
<i>vlan_id</i>	The service VLAN ID number. The valid range is 1 to 4094.
<i>level_num</i>	The MEG level number for the service VLAN. The valid range is 0 to 7.
<i>guard-timer</i>	The guard timer value, in centi-secs, for the ring node.
<i>wtr-timer</i>	The wait-to-restore timer value, in minutes, for the Ring Protection Link (RPL) node.
enable	Administratively enables the ERP sub-ring.
disable	Administratively disables the ERP sub-ring.

Defaults

parameter	default
<i>guard_timer</i>	50
<i>wtr_timer</i>	5
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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.
- ERP is not supported on mobile ports, mirroring ports, link aggregate member ports, high availability ports, Multicast VLAN receiver ports (ERP is supported on Multicast VLAN sender ports only), VLAN Stacking user network interface (UNI) ports, or RRSTP ring ports.

- If a port is tagged with the service VLAN ID or the service VLAN is the default VLAN for the port, the port is not eligible to become an ERP ring port.
- Specify an existing VLAN ID for the service VLAN ID. Use the same VLAN ID and level number for the service VLAN on each switch that participates in the ERP ring.
- If the ERP switch participates in an Ethernet OAM Maintenance Domain (MD), configure the ERP service VLAN to use the same level number that is used for the Ethernet OAM MD.
- Specify a static VLAN ID for the ERP service VLAN; dynamic VLANs are not configurable as service VLANs.
- The service VLAN can belong to only one ERP ring at a time. A maximum of four rings are allowed per switch.
- The specified service VLAN ID must not participate in a Spanning Tree instance that is associated with non-ERP VLANs. Ideally, change the Spanning Tree configuration for the VLAN ID prior to using this command.
- An ERP ring port can belong to only one ERP ring at a time.
- An ERP type NNI-SVLAN binding must be created before establishing an ERP ring on that SVLAN-NNI binding.

Examples

```
-> erp-ring 1 sub-ring-port 1/1 service-vlan 10 level 2 enable
-> erp-ring 2 sub-ring-port linkagg 1 port2 2/10 service-vlan 20 level 2
-> no erp-ring 2
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.
ethernet-service svlan nni	Creates a NNI-SVLAN binding.

MIB Objects

```
alaErpRingTable
  alaErpRingId
  alaErpRingServiceVid
  alaErpRingMEGLevel
  alaErpRingStatus
  alaErpRingPort1
  alaErpRingPort2
  alaErpRingWaitToRestore
  alaErpRingGuardTimer
  alaErpRingRowStatus
```

erp-ring virtual-channel

Enables or disables an Ethernet Ring Protection (ERP) Ring Virtual Channel.

erp-ring *ring_id* **virtual-channel** [**enable** | **disable**]

Syntax Definitions

<i>ring_id</i>	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 10K, 6900

Usage Guidelines

- The specified ring identification number must be unique within a switch.
- The ring identified by Ring ID must be created before configuring the virtual channel state for ring node.

Examples

```
-> erp-ring 2 virtual-channel disable
-> erp-ring 1 virtual-channel enable
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects`alaErpRingTable``alaErpRingId``alaErpRingVirtualChannel`

erp-ring revertive

Enables or Disables revertive mode on the specified node.

erp-ring *ring_id* revertive [enable | disable]

Syntax Definitions

<i>ring_id</i>	The ERP ring ID number. The valid range is 1 to 2147483647.
enable	Administratively enables Revertive Mode. Now, if the RPL is unblocked due to a failure within the ring, the RPL automatically reverts to the “Blocked” state when the failed link recovers.
disable	Administratively Disables Revertive Mode. Now, if the RPL is unblocked due to a failure within the ring, the RPL does not automatically revert to “Blocked” state when the failed link recovers.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

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 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
erp-ring clear	Clears any pending state (for example, non-revertive restoring).
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable  
  alaErpRingId  
  alaErpRingRevertive
```

erp-ring clear

Clears any pending state (for example, non-revertive restoring).

erp-ring *ring_id* clear

Syntax Definitions

<i>ring_id</i>	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 10K, 6900

Usage Guidelines

The specified ring identification number must be unique within a switch.

Examples

```
-> erp-ring 1 clear
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpRingTable  
  alaErpRingId  
  alaErpRingClearAction
```

erp-ring ethoam-event

Configures a ring port to accept a “loss of connectivity” event from Ethernet OAM for a remote endpoint.

```
erp-ring ring_id ethoam-event {slot/port | linkagg agg_num} remote-endpoint mep_id
```

```
no erp-ring ring_id ethoam-event {slot/port | linkagg agg_num}
```

Syntax Definitions

<i>ring_id</i>	The ERP ring ID number. The valid range is 1 to 2147483647.
<i>slot/port</i>	The slot number for the module and the physical port number on that module.
<i>agg_num</i>	The link aggregate ID number.
<i>mep_id</i>	The remote endpoint ID.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The specified ring identification number must be unique within a switch.

Examples

```
-> erp-ring 1 ethoam-event 1/1 remote-endpoint 10  
-> erp-ring 1 ethoam-event linkagg 1 remote-endpoint 10
```

Release History

Release 7.3.1; command introduced.

Related Commands

erp-ring	Creates an Ethernet Ring Protection (ERP) ring.
erp-ring sub-ring	Creates an Ethernet Ring Protection (ERP) ring sub ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

alaErpRingTable

 alaErpRingId

 alaErpRingPortIfIndex

 alaErpRingPortEthOAMEvent

 alaErpRingPortRmepId

clear erp statistics

Clears ERP statistics for all rings, a specific ring, or a specific ring port.

clear erp statistics [**ring** *ring_id* [**port** *slot/port* | **linkagg** *agg_num*]]

Syntax Definitions

<i>ring_id</i>	An existing ERP ring ID number. The valid range is 1 to 2147483647.
<i>slot/port</i>	The slot number for the module and the physical port number on that module.
<i>agg_num</i>	The link aggregate ID number.

Defaults

By default, statistics are cleared for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Enter a ring ID to clear the statistics for a specific ring.
- Enter a ring ID and a ring port number or link aggregate ID to clear the statistics for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.
- The specified port must belong to the ring identified by the ring ID.

Examples

```
-> clear erp statistics
-> clear erp statistics ring 5
-> clear erp statistics ring 5 port 1/2
-> clear erp statistics ring 5 linkagg 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

erp-ring	Configures an ERP ring.
show erp	Displays the ERP ring configuration for the switch.
show erp statistics	Displays ERP ring statistics.

MIB Objects

```
alaErpClearStats  
alaErpRingTable  
    alaErpRingId  
    alaErpRingClearStats  
alaErpRingPortTable  
    alaErpRingPortIfIndex  
    alaErpRingPortClearStats
```

show erp

Displays the ERP configuration information for all rings, a specific ring, or for a specific ring port.

show erp [**ring** *ring_id*] [**port** *slot/port* | **linkagg** *agg_num*]

Syntax Definitions

<i>ring_id</i>	An existing ERP ring ID number. The valid range is 1 to 2147483647.
<i>slot/port</i>	The slot number for the module and the physical port number on that module.
<i>agg_num</i>	The link aggregate ID number.

Defaults

By default, configuration information is displayed for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Enter a ring ID to display the configuration for a specific ring.
- Enter a ring port number or a link aggregate ID to display the configuration for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.

Examples

```
-> show erp
```

```
Legends: *   to Inactive Configuration
          WTR to Wait To Restore
          MEG to Maintenance Entity Group
```

Ring ID	Ring Port1	Ring Port2	Ring Status	Serv VLAN	WTR Timer (min)	Guard Timer (csec)	MEG Level	Ring State	Ring Node
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

```
-> show erp ring 1
```

```
Legend: *   to Inactive Configuration
```

```
Ring Id           : 1,
Ring Port1       : 1/15,
```

```

Ring Port2           : 1/1,
Ring Status          : enabled,
Service VLAN         : 4094,
WTR Timer (min)     : 3,
Guard Timer (centi-sec) : 50,
MEG Level            : 2,
Ring State           : idle,
Ring Node Type       : rpl,
RPL Port             : 1/1,
Last State Change    : SUN DEC 25 06:50:17 2016 (sysUpTime 00h:01m:31s)

```

output definitions

Ring ID	The ERP ring ID number.
Ring Ports	The slot and port number of the ring ports.
Ring Status	The ring status (enabled or disabled).
Service VLAN	The Service VLAN ID.
WTR Timer	The wait-to-restore timer value in minutes for RPL node.
Guard Timer	The guard timer value in centi-secs for the ring node.
MEG Level	The Service VLAN Management Entity Group (MEG) level.
Ring State	Indicates the state of the ring.
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
Legend: * to Inactive Configuration

```

```

Ring-Id : 1
  Ring Port Status   : forwarding,
  Ring Port Type     : non-rpl,
  Ethoam Event       : disabled

```

```

-> show erp port 1/1
Legend: * to Inactive Configuration

```

```

Ring Id : 1
  Ring Port Status   : blocking,
  Rint Port Type     : RPL,
  Ethoam Event       : enabled,
  Rmepid             : 10

```

output definitions

Ring ID	The ERP ring ID number.
Ring Port Status	The status of the ring port (blocking or forwarding).
Ring Port Type	The type of ring port (RPL or non-RPL).
Ethoam Event	Indicates whether or not the ring port will accept Ethernet OAM loss of connectivity events (enabled or disabled).
Rmepid	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 7.1.1; command introduced.

Related Commands

[show erp statistics](#) Displays ERP ring statistics.

MIB Objects

```
alaErpRingId
  alaErpRingStatus
  alaErpRingServiceVid
  alaErpRingMEGLevel
  alaErpRingPort1
  alaErpRingPort2
  alaErpRingPortIfIndex
  alaErpRingState
  alaErpRingPortStatus
  alaErpRingPortType
  alaErpRingPortEthOAMEvent
  alaErpRingPortRmepId
  alaErpRingWaitToRestoreTimer
  alaErpRingGuardTimer
  alaErpRingLastStateChange
  alaErpRingTimeToRevert
```

show erp statistics

Displays the ERP statistics for all rings, a specific ring, or a specific ring port.

```
show erp statistics [ring ring_id [port slot/port | linkagg agg_num]]
```

Syntax Definitions

<i>ring_id</i>	An existing ERP ring ID number. The valid range is 1 to 2147483647.
<i>slot/port</i>	The slot number for the module and the physical port number on that module.
<i>agg_num</i>	The link aggregate ID number.

Defaults

By default, statistics are displayed for all ERP rings in the switch configuration.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Enter a ring ID to display the statistics for a specific ring.
- Enter a ring ID and a ring port number or link aggregate ID to display the statistics for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.
- The specified port must belong to the ring identified by the ring ID.

Examples

```
-> show erp statistics
Legends: R-APS   to Ring Automatic Protection Switching
         RPL     to 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 : 4322,
      Recv : 0,
      Drop : 0
    Invalid R-APS PDUs
      Recv : 0
```

```
Ring Port : 1/1
  Signal Fail PDUs
    Sent : 6,
    Recv : 0,
    Drop : 0
  No Request PDUs
    Sent : 37,
    Recv : 38,
    Drop : 0
  No Request RPL Block PDUs
    Sent : 4322,
    Recv : 0,
    Drop : 0
  Invalid R-APS PDUs
    Recv : 0

Ring-Id : 2
  Ring Port : 6/7
    Signal Fail PDUs
      Sent : 6,
      Recv : 0,
      Drop : 0
    No Request PDUs
      Sent : 16,
      Recv : 14,
      Drop : 0
    No Request RPL Block PDUs
      Sent : 4347,
      Recv : 0,
      Drop : 4341
    Invalid R-APS PDUs
      Recv : 0

-> show erp statistics ring 3
Legends: R-APS  to Ring Automatic Protection Switching
         RPL    to 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 to Ring Automatic Protection Switching
 RPL to 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.
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 7.1.1; command introduced.

Related Commands

<code>show erp</code>	Displays the ERP ring configuration for the switch.
<code>clear erp statistics</code>	Clears ERP ring statistics.

MIB Objects

```
alaERPClearStats  
alaERPRingClearStats  
alaErpRingPortClearStats  
alaErpRingId  
  alaErpRingPortIfIndex  
  alaErpStatsSignalFailPduTx  
  alaErpStatsSignalFailPduRx  
  alaErpStatsSignalFailPduDrop  
  alaErpStatsNoRequestPduTx  
  alaErpStatsNoRequestPduRx  
  alaErpStatsNoRequestPduDrop  
  alaErpStatsRPLBlockPDUTx  
  alaErpStatsRPLBlockPDURx  
  alaErpStatsRPLBlockPDUDrop  
  alaErpStatsPDUErr
```

11 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.

A summary of the available commands is listed here:

- mvrp**
- mvrp port**
- 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 mvrp vlan-restrictions**
- show mvrp vlan-restrictions**
- mvrp clear-statistics**

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 10K, 6900

Usage Guidelines

- Disabling MVRP globally deletes 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 per-VLAN mode.

Examples

```
-> mvrp enable  
-> mvrp disable
```

Release History

Release 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

Related Commands

[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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	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 10K, 6900

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 must 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, VLAN Stacking User ports) do not support MVRP.

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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>agg_num</i>	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 10K, 6900

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 must 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 must be created.

Examples

```
-> mvrp linkagg 10 enable
-> mvrp linkagg 10 disable
-> mvrp linkagg 2-5 enable
-> mvrp linkagg 1-5 disable
```

Release History

Release 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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 maximum-vlan

Configures the maximum number of dynamic VLANs that can be created by MVRP.

mvrp maximum-vlan *vlan_limit*

Syntax Definitions

vlan_limit The maximum number of VLANs to be created by MVRP. The valid range is 32–4094.

Defaults

The default value is 256.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command can be used even when MVRP is not enabled on the switch. However, MVRP must 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 re-enabled on the switch. The VLANs learnt earlier are retained if this operation is not performed.

Examples

```
-> mvrp maximum-vlan 100
```

Release History

Release 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

Related Commands

- [show mvrp configuration](#) Displays the global configuration for MVRP.
[show mvrp vlan-restrictions](#) 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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	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 VLANs created earlier is de-registered.

Defaults

parameter	default
normal fixed forbidden	normal

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

To use the *agg_num* parameter, the link aggregate group must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	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 10K, 6900

Usage Guidelines

To use the *agg_num* parameter, the link aggregate group must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	The number corresponding to the aggregate group.
<i>timer-value</i>	Specifies the value of the join timer in milliseconds. The valid range is 250 milliseconds to 1073741773 milliseconds.

Defaults

parameter	default
<i>timer-value</i>	600 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- To use the *agg_num* parameter, the link aggregate group must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	The number corresponding to the aggregate group.
<i>timer-value</i>	Specifies the value of the Leave Timer in milliseconds. The valid range is 750 milliseconds to 2147483647 milliseconds.

Defaults

parameter	default
<i>timer-value</i>	1800 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- Leave timer value must be greater than or equal to twice the Join timer value, plus six times the timer resolution (16.66 milliseconds). Leave timer must be at least be greater than twice the join timer plus 100 milliseconds.
- To use the *agg_num* parameter, the link aggregate group must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	The number corresponding to the aggregate group.
<i>timer-value</i>	Specifies the value of the LeaveAll Timer in milliseconds. The valid range is 750 milliseconds to 2147483647 milliseconds.

Defaults

parameter	default
<i>timer-value</i>	30000 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- Leaveall timer value must 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 must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	The number corresponding to the aggregate group.
<i>timer-value</i>	Specifies the value of the Periodic Timer in seconds. The valid range is between 1 to 2147483647 milliseconds.

Defaults

parameter	default
<i>timer-value</i>	<i>1 second</i>

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- To use the *agg_num* parameter, the link aggregate group must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	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 is disabled on all the ports.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

To use the *agg_num* parameter, the link aggregate group must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	The number corresponding to the aggregate group.
<i>vlan_list</i>	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 10K, 6900

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 must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>agg_num</i>	The number corresponding to the aggregate group.
<i>vlan_list</i>	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 10K, 6900

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 must 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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

<i>agg_num</i>	The number corresponding to the aggregate group.
<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>vlan_list</i>	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 10K, 6900

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.

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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show mvrp configuration
MVRP Enabled : yes,
Maximum VLAN Limit : 256
```

output definitions

MVRP Enabled	Indicates whether MVRP is globally enabled.
Maximum VLAN Limit	The maximum number of VLANs that can be learned by MVRP in the system.

Release History

Release 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

Related Commands

mvrp	Enables or disables MVRP globally on the switch.
mvrp maximum-vlan	Configures the maximum number of dynamic VLANs that can be created by MVRP.

MIB Objects

```
alaMvrpGlobalStatus
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*]} [**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 To display only the enabled ports.

disable To display only the disabled ports.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

-> show mvrp port enable

Port	Join Timer (msec)	Leave Timer (msec)	LeaveAll Timer (msec)	Periodic Timer (sec)	Registration Mode	Applicant Mode	Periodic Tx Status
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 disable

Port	Join Timer (msec)	Leave Timer (msec)	LeaveAll Timer (msec)	Periodic Timer (sec)	Registration Mode	Applicant Mode	Periodic Tx Status
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 Timer (msec)	Leave Timer (msec)	LeaveAll Timer (msec)	Periodic Timer (sec)	Registration Mode	Applicant Mode	Periodic Tx Status
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 Timer (msec)	Leave Timer (msec)	LeaveAll Timer (msec)	Periodic Timer (sec)	Registration Mode	Applicant Mode	Periodic Tx Status
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 enable

ERROR: MVRP is disabled on port 1/1

output definitions

Port	Displays the slot and 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.
Periodic Tx Status	The transmission status of MVRP, enable or disable .

Release History

Release 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

Related Commands

mvrp port

Enables or disables MVRP on specific ports on the switch.

mvrp

Configures VLAN dynamic registration mode to 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

<i>agg_num</i>	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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show mvrp linkagg 1-3
```

Port	Status	Join Timer (msec)	Leave Timer (msec)	LeaveAll Timer (msec)	Periodic Timer (sec)	Registration Mode	Applicant Mode	Periodic Tx Status
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 disable
```

```
ERROR: MVRP is enabled on linkagg 0/1
```

Note. In the command output shown below, the MVRP status is not displayed as the command is only for enabled ports and link aggregates.

```
-> show mvrp linkagg 10 enable
```

```
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
```

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.
Periodic Tx Status	The transmission status of MVRP, enable or disable

Release History

Release 7.2.1; command introduced.
 Release 7.2.1.R02; Support for OS10K added.

Related Commands

mvrp port Enables or disables MVRP on specific ports on the switch.

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

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

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 (msec)	Leave Timer (msec)	LeaveAll Timer (sec)	Periodic Timer (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.

output definitions (continued)

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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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/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.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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,
Join 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,
Join 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,
Join 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.

output definitions (continued)

New Transmitted	The number of new MVRP messages sent by the switch.
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 7.2.1; command introduced.
 Release 7.2.1.R02; Support for OS10K added.

Related Commands

- show mvrp configuration** Clears MVRP statistics for all 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
  alaMvrpPortStatsTotalPDURceived
  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/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.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

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 and port number.
Last PDU origin	The source MAC address of the last PDU message received on the specific port.

Release History

Release 7.2.1; command introduced.

Release 7.2.1.R02; Support for OS10K added.

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 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

<i>agg_num</i>	The number corresponding to the aggregate group.
<i>slot/port</i>	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 10K, 6900

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 Registration	Restricted Registration	Restricted 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.

output definitions (continued)

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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

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
```

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/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.

Defaults

If no ports are specified, the MVRP statistics are deleted for all the ports.

Platforms Supported

OmniSwitch 10K, 6900

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 7.2.1; command introduced.
Release 7.2.1.R02; Support for OS10K added.

Related Commands

[show mvrp statistics](#) Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

```
alaMvrpGlobalClearStats
  alaMvrpPortStatsTable
  alaMvrpPortStatsClearStats
```

12 802.1AB Commands

802.1AB is an IEEE standard for exchanging information with neighboring devices and maintaining a database of it. The information is exchanged as an LLDPDU (Link Layer Discovery Protocol Data Unit) in TLV (Time, Length, Value) format. This chapter details configuring and monitoring 802.1AB on a switch.

Alcatel-Lucent's 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

A summary of available commands is listed here:

lldp transmit interval
lldp transmit hold-multiplier
lldp transmit delay
lldp reinit delay
lldp notification interval
lldp lldpdu
lldp notification
lldp tlv management
lldp tlv dot1
lldp tlv dot3
lldp tlv med
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

Configuration procedures for 802.1AB are explained in “Configuring 802.1AB,” *OmniSwitch 10K Network Configuration Guide*.

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
<i>seconds</i>	30

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The LLDP protocol must be enabled before using this command.

Examples

```
-> lldp transmit interval 40
```

Release History

Release 7.1.1; command introduced.

Related Commands

- [lldp transmit hold-multiplier](#) Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.
- [show lldp local-system](#) Displays local system information.

MIB Objects

```
lldpConfiguration  
  lldpMessageTxInterval
```

lldp transmit hold-multiplier

Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.

lldp transmit hold-multiplier *num*

Syntax Definitions

num The transmit hold multiplier value. The valid range is 2-10.

Defaults

parameter	default
<i>num</i>	4

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

[lldp transmit interval](#) Sets the transmit time interval for LLDPDUs.
[show lldp local-system](#) Displays local system information.

MIB Objects

lldpConfiguration
lldpMessageTxHoldMultiplier

lldp transmit delay

Sets the minimum time interval between successive LLDPDUs transmitted.

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
<i>seconds</i>	2

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

[lldp transmit interval](#) Sets the transmit time interval for LLDPDUs.
[show lldp local-system](#) Displays local system information.

MIB Objects

lldpConfiguration
 lldpTxDelay

lldp reinit delay

Sets the time interval that must elapse before the current 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
<i>seconds</i>	2

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The LLDP protocol must be enabled before using this command.

Examples

```
-> lldp reinit delay 4
```

Release History

Release 7.1.1; 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
<i>seconds</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The LLDP protocol and notification must be enabled before using this command.
- In a specified interval, it is not possible to generate more than one notification-event.

Examples

```
-> lldp notification interval 25
```

Release History

Release 7.1.1; command introduced.

Related Commands

- [lldp notification](#) Specifies the switch to control per port notification status about the remote device change.
- [show lldp local-system](#) Displays local system information.

MIB Objects

```
lldpConfiguration  
  lldpNotificationInterval
```

lldp lldpdu

Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

lldp {port *slot/port* [-port] | slot *slot* / chassis} lldpdu {tx | rx | tx-and-rx | disable}

Syntax Definitions

<i>slot/port</i>	Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>slot</i>	The slot number for a specific module.
chassis	Specifies the whole chassis.
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 10K, 6900

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 port 1/2 lldpdu tx-and-rx
-> lldp slot 3 lldpdu tx
-> lldp chassis lldpdu disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

lldp lldpdu

Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

lldp notification

Specifies the switch to control per port notification status about the remote device change.

MIB Objects

lldpPortConfigTable

 lldpPortConfigPortNum

 lldpPortConfigAdminStatus

lldp notification

Specifies the switch to control per port notification status about the remote device change.

lldp {port *slot/port*[-*port*] | slot *slot* / chassis} notification {enable | disable}

Syntax Definitions

<i>slot/port</i>	Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>slot</i>	The slot number for a specific module.
enable	Enables the notification of local system MIB changes.
disable	Disables the notification.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 port 1/2 notification enable
-> lldp slot 1 notification disable
```

Release History

Release 7.1.1; 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

Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

MIB Objects

lldpPortConfigTable

 lldpPortConfigPortNum

 lldpPortConfigNotificationEnable

lldp tlv management

Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

lldp {port *slot/port* [-*port*] | slot *slot* / chassis} **tlv management** {port-description | system-name | system-description | system-capabilities | management-address} {enable | disable}

Syntax Definitions

<i>slot/port</i>	Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>slot</i>	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 10K, 6900

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 port 1/2 tlv management port-description enable
-> lldp slot 2 tlv management management-address enable
-> lldp slot 3 tlv management system-name disable
-> lldp chassis tlv management system-capabilities enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
show lldp local-system	Displays local system information.
show lldp local-port	Displays 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

Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

lldp {port *slot/port* [-*port*] | slot *slot* / chassis} **tlv dot1** {port-vlan | vlan-name} {enable | disable}

Syntax Definitions

<i>slot/port</i>	Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>slot</i>	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 10K, 6900

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 port 5/1 tlv dot1 port-vlan enable
-> lldp slot 3 tlv dot1 vlan-name enable
-> lldp slot 3 tlv dot1 vlan-name disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
show lldp statistics	Displays per port statistics.
show lldp local-port	Displays per port information.

MIB Objects

```
lldpPortConfigTable
  lldpPortConfigPortNum
lldpXdot1ConfigPortVlanTable
  lldpXdot1ConfigPortVlanTxEnable
lldpXdot1ConfigVlanNameTable
  lldpXdot1ConfigVlanNameTxEnable
```

lldp tlv dot3

Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.

lldp {port *slot/port* [-port]| slot *slot* / chassis} **tlv dot3 mac-phy** {enable | disable}

Syntax Definitions

<i>slot/port</i>	Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>slot</i>	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 10K, 6900

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 port 2/4 tlv dot3 mac-phy enable
-> lldp slot 2 tlv dot3 mac-phy disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot1	Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.
show lldp statistics	Displays per port statistics.

MIB Objects

```
lldpPortConfigTable  
  lldpPortConfigPortNum  
lldpXdot3PortConfigTable  
  lldpXdot3PortConfigTLVsTxEnable
```

lldp tlv med

Specifies the switch to control per port LLDP-MED (Media Endpoint Device) TLVs to be incorporated in the LLDPDU.

lldp {port *slot/port* [-*port*] | slot *slot* / chassis} tlv med {power | capability} {enable | disable}

Syntax Definitions

<i>slot/port</i>	Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>slot</i>	The slot number for a specific module.
capability	Enables or disables transmission of LLDP-MED capabilities TLV in LLDPDU.
enable	Enables LLDP-MED TLV LLDPDU transmission.
disable	Disables LLDP-MED TLV LLDPDU transmission.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 will be lost.

Examples

```
-> lldp 4/4 tlv med power enable
-> lldp 4/3 tlv med capability enable
-> lldp 4 tlv med power disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot1	Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.
lldp tlv dot3	Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.

MIB Objects

```
lldpPortConfigTable  
  lldpPortConfigPortNum  
lldpXMedPortConfigTable  
  lldpXMedPortConfigTLVsTxEnable
```

show lldp system-statistics

Displays system-wide statistics.

show lldp system-statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

lldp notification

Specifies the switch to control per port notification status about the remote device change.

lldp notification interval

Sets the time interval that must elapse before a notification about the local system MIB change is generated.

MIB Objects

lldpStatistics

lldpStatsRemTablesLastChangeTime

lldpStatsRemTablesInserts

lldpStatsRemTablesDeletes

lldpStatsRemTablesDrops

lldpStatsRemTablesAgeouts

show lldp statistics

Displays per port statistics.

show lldp [port slot/port [-port]] statistics

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).

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the slot/port option is not specified, statistics for the chassis is displayed.
- If the statistics are zero they are not displayed.

Examples

-> show lldp statistics

Slot/Port	Tx	LLDPDU Rx	Errors	LLDPDU Discards	TLV Unknown	TLV Discards	Device 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 7.1.1; command introduced.

Related Commands

lldp lldpdu

Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

lldp tlv management

Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

MIB Objects

lldpStatsTxPortTable

 lldpStatsTxPortNum

 lldpStatsTxPortFramesTotal

lldpStatsRxPortTable

 lldpStatsRxPortNum

 lldpStatsRxPortFramesDiscardedTotal

 lldpStatsRxPortFramesErrors

 lldpStatsRxPortFramesTotal

 lldpStatsRxPortTLVsDiscardedTotal

 lldpStatsRxPortTLVsUnrecognizedTotal

 lldpStatsRxPortAgeoutsTotal

show lldp local-system

Displays local system information.

show lldp local-system

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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             = Kite2_Stack_of_2,
  System Description      = 6.3.1.636.R01 Development, September 07, 2007.,
  Capabilites Supported   = Bridge, Router,
  Capabilites Enabled     = Bridge, Router,
  LLDPDU Transmit Interval = 30 seconds,
  TTL Hold Multiplier     = 4,
  LLDPDU Transmit Delay   = 2 seconds,
  Reintialization Delay   = 2 seconds,
  MIB Notification Interval = 5 seconds
  Management Address Type = 1 (IPv4),
  Management IP Address   = 10.255.11.100,
```

output definitions

Chassis ID Subtype	The subtype that describe chassis ID.
Chassis ID	The chassis ID (MAC address).
System Name	The name of the system.
System Description	The description of the system.
Capabilites Supported	The capabilities of the system.
Capabilites Enabled	The enabled capabilities of the system.
LLDPDU Transmit Interval	The LLDPDU transmit interval.
TTL Hold Multiplier	The hold multiplier used to calculate TTL.

output definitions (continued)

LLDPDU Transmit Delay	The minimum transmit time between successive LLDPDUs.
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.
Management Address Type	The type of management address used in LLDPDU.
Management IP Address	The management IP address. The loopback0 IP address is configured for the management IP address to be transmitted.

Release History

Release 7.1.1; command introduced.

Related Commands

lldp reinit delay	Sets the time interval that must elapse before the current status of a port is reinitialized after a status change.
lldp transmit hold-multiplier	Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.
lldp transmit delay	Sets the minimum time interval between successive LLDPDUs transmitted.

MIB Objects

```
lldpLocalSystemData
  lldpLocChassisIdSubtype
  lldpLocChassisId
  lldpLocSysName
  lldpLocSysDesc
  lldpLocSysCapSupported
  lldpLocSysEnabled
lldpPortConfigTable
  lldpMessageTxInterval
  lldpMessageTXHoldMultiplier
  lldpTxDelay
  lldpReinitDelay
  lldpNotificationInterval
lldpLocManAddrTable
  lldpLocManAddrSubtype
  lldpLocManAddr
```

show lldp local-port

Displays per port information.

show lldp [port slot/port [-port]] slot slot] local-port

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).

slot The slot number for a specific module.

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show lldp local-port
Local Slot 1/Port 1 LLDP Info:
  Port ID           = 1001 (Locally assigned),
  Port Description   = Alcatel 1/1 6.3.1.636.R01,
Local Slot 1/Port 2 LLDP Info:
  Port ID           = 1002 (Locally assigned),
  Port Description   = Alcatel 1/2 6.3.1.636.R01,
Local Slot 1/Port 3 LLDP Info:
  Port ID           = 1003 (Locally assigned),
  Port Description   = Alcatel 1/3 6.3.1.636.R01,
Local Slot 1/Port 4 LLDP Info:
  Port ID           = 1004 (Locally assigned),
  Port Description   = Alcatel 1/4 6.3.1.636.R01,
Local Slot 1/Port 5 LLDP Info:
  Port ID           = 1005 (Locally assigned),
  Port Description   = Alcatel 1/5 6.3.1.636.R01,
Local Slot 1/Port 6 LLDP Info:
  Port ID           = 1006 (Locally assigned),
  Port Description   = Alcatel 1/6 6.3.1.636.R01,
Local Slot 1/Port 7 LLDP Info:
  Port ID           = 1007 (Locally assigned),
  Port Description   = Alcatel 1/7 6.3.1.636.R01,
Local Slot 1/Port 8 LLDP Info:
  Port ID           = 1008 (Locally assigned),
  Port Description   = Alcatel 1/8 6.3.1.636.R01,
Local Slot 1/Port 9 LLDP Info:
  Port ID           = 1009 (Locally assigned),
  Port Description   = Alcatel 1/9 6.3.1.636.R01,
```

```
Local Slot 1/Port 10 LLDP Info:
  Port ID                = 1010 (Locally assigned),
  Port Description        = Alcatel 1/10 6.3.1.636.R01,
Local Slot 1/Port 11 LLDP Info:
  Port ID                = 1011 (Locally assigned),
  Port Description        = Alcatel 1/11 6.3.1.636.R01,
Local Slot 1/Port 12 LLDP Info:
  Port ID                = 1012 (Locally assigned),
  Port Description        = Alcatel 1/12 6.3.1.636.R01,
Local Slot 1/Port 13 LLDP Info:
  Port ID                = 1013 (Locally assigned),
  Port Description        = Alcatel 1/13 6.3.1.636.R01,
Local Slot 1/Port 14 LLDP Info:
  Port ID                = 1014 (Locally assigned),
  Port Description        = Alcatel 1/14 6.3.1.636.R01,
Local Slot 1/Port 15 LLDP Info:
  Port ID                = 1015 (Locally assigned),
  Port Description        = Alcatel 1/15 6.3.1.636.R01,
Local Slot 1/Port 16 LLDP Info:
  Port ID                = 1016 (Locally assigned),
  Port Description        = Alcatel 1/16 6.3.1.636.R01,
Local Slot 1/Port 17 LLDP Info:
  Port ID                = 1017 (Locally assigned),
  Port Description        = Alcatel 1/17 6.3.1.636.R01,
Local Slot 1/Port 18 LLDP Info:
  Port ID                = 1018 (Locally assigned),
  Port Description        = Alcatel 1/18 6.3.1.636.R01,
Local Slot 1/Port 19 LLDP Info:
  Port ID                = 1019 (Locally assigned),
  Port Description        = Alcatel 1/19 6.3.1.636.R01,
Local Slot 1/Port 20 LLDP Info:
  Port ID                = 1020 (Locally assigned),
  Port Description        = Alcatel 1/20 6.3.1.636.R01,
Local Slot 1/Port 21 LLDP Info:
  Port ID                = 1021 (Locally assigned),
  Port Description        = Alcatel 1/21 6.3.1.636.R01,
Local Slot 1/Port 22 LLDP Info:
  Port ID                = 1022 (Locally assigned),
  Port Description        = Alcatel 1/22 6.3.1.636.R01,
Local Slot 1/Port 23 LLDP Info:
  Port ID                = 1023 (Locally assigned),
  Port Description        = Alcatel 1/23 6.3.1.636.R01,
Local Slot 1/Port 24 LLDP Info:
  Port ID                = 1024 (Locally assigned),
  Port Description        = Alcatel 1/24 6.3.1.636.R01,
Local Slot 1/Port 25 LLDP Info:
  Port ID                = 1025 (Locally assigned),
  Port Description        = ,
Local Slot 1/Port 26 LLDP Info:
  Port ID                = 1026 (Locally assigned),
  Port Description        = ,
Local Slot 2/Port 1 LLDP Info:
  Port ID                = 2001 (Locally assigned),
  Port Description        = Alcatel 2/1 6.3.1.636.R01,
Local Slot 2/Port 2 LLDP Info:
  Port ID                = 2002 (Locally assigned),
  Port Description        = Alcatel 2/2 6.3.1.636.R01,
Local Slot 2/Port 3 LLDP Info:
  Port ID                = 2003 (Locally assigned),
```

```
Port Description          = Alcatel 2/3 6.3.1.636.R01,
Local Slot 2/Port 4 LLDP Info:
  Port ID                 = 2004 (Locally assigned),
  Port Description        = Alcatel 2/4 6.3.1.636.R01,
Local Slot 2/Port 5 LLDP Info:
  Port ID                 = 2005 (Locally assigned),
  Port Description        = Alcatel 2/5 6.3.1.636.R01,
Local Slot 2/Port 6 LLDP Info:
  Port ID                 = 2006 (Locally assigned),
  Port Description        = Alcatel 2/6 6.3.1.636.R01,
Local Slot 2/Port 7 LLDP Info:
  Port ID                 = 2007 (Locally assigned),
  Port Description        = Alcatel 2/7 6.3.1.636.R01,
Local Slot 2/Port 8 LLDP Info:
  Port ID                 = 2008 (Locally assigned),
  Port Description        = Alcatel 2/8 6.3.1.636.R01,
Local Slot 2/Port 9 LLDP Info:
  Port ID                 = 2009 (Locally assigned),
  Port Description        = Alcatel 2/9 6.3.1.636.R01,
Local Slot 2/Port 10 LLDP Info:
  Port ID                 = 2010 (Locally assigned),
  Port Description        = Alcatel 2/10 6.3.1.636.R01,
Local Slot 2/Port 11 LLDP Info:
  Port ID                 = 2011 (Locally assigned),
  Port Description        = Alcatel 2/11 6.3.1.636.R01,
Local Slot 2/Port 12 LLDP Info:
  Port ID                 = 2012 (Locally assigned),
  Port Description        = Alcatel 2/12 6.3.1.636.R01,
Local Slot 2/Port 13 LLDP Info:
  Port ID                 = 2013 (Locally assigned),
  Port Description        = Alcatel 2/13 6.3.1.636.R01,
Local Slot 2/Port 14 LLDP Info:
  Port ID                 = 2014 (Locally assigned),
  Port Description        = Alcatel 2/14 6.3.1.636.R01,
Local Slot 2/Port 15 LLDP Info:
  Port ID                 = 2015 (Locally assigned),
  Port Description        = Alcatel 2/15 6.3.1.636.R01,
Local Slot 2/Port 16 LLDP Info:
  Port ID                 = 2016 (Locally assigned),
  Port Description        = Alcatel 2/16 6.3.1.636.R01,
Local Slot 2/Port 17 LLDP Info:
  Port ID                 = 2017 (Locally assigned),
  Port Description        = Alcatel 2/17 6.3.1.636.R01,
Local Slot 2/Port 18 LLDP Info:
  Port ID                 = 2018 (Locally assigned),
  Port Description        = Alcatel 2/18 6.3.1.636.R01,
Local Slot 2/Port 19 LLDP Info:
  Port ID                 = 2019 (Locally assigned),
  Port Description        = Alcatel 2/19 6.3.1.636.R01,
Local Slot 2/Port 20 LLDP Info:
  Port ID                 = 2020 (Locally assigned),
  Port Description        = Alcatel 2/20 6.3.1.636.R01,
Local Slot 2/Port 21 LLDP Info:
  Port ID                 = 2021 (Locally assigned),
  Port Description        = Alcatel 2/21 6.3.1.636.R01,
Local Slot 2/Port 22 LLDP Info:
  Port ID                 = 2022 (Locally assigned),
  Port Description        = Alcatel 2/22 6.3.1.636.R01,
Local Slot 2/Port 23 LLDP Info:
```

```
Port ID = 2023 (Locally assigned),
Port Description = Alcatel 2/23 6.3.1.636.R01,
Local Slot 2/Port 24 LLDP Info:
Port ID = 2024 (Locally assigned),
Port Description = Alcatel 2/24 6.3.1.636.R01,
Local Slot 2/Port 25 LLDP Info:
Port ID = 2025 (Locally assigned),
Port Description = Alcatel 2/25 6.3.1.636.R01,
Local Slot 2/Port 26 LLDP Info:
Port ID = 2026 (Locally assigned),
Port Description = Alcatel 2/26 6.3.1.636.R01,
Local Slot 2/Port 27 LLDP Info:
Port ID = 2027 (Locally assigned),
Port Description = Alcatel 2/27 6.3.1.636.R01,
Local Slot 2/Port 28 LLDP Info:
Port ID = 2028 (Locally assigned),
Port Description = Alcatel 2/28 6.3.1.636.R01,
Local Slot 2/Port 29 LLDP Info:
Port ID = 2029 (Locally assigned),
Port Description = Alcatel 2/29 6.3.1.636.R01,
Local Slot 2/Port 30 LLDP Info:
Port ID = 2030 (Locally assigned),
Port Description = Alcatel 2/30 6.3.1.636.R01,
Local Slot 2/Port 31 LLDP Info:
Port ID = 2031 (Locally assigned),
Port Description = Alcatel 2/31 6.3.1.636.R01,
Local Slot 2/Port 32 LLDP Info:
Port ID = 2032 (Locally assigned),
Port Description = Alcatel 2/32 6.3.1.636.R01,
Local Slot 2/Port 33 LLDP Info:
Port ID = 2033 (Locally assigned),
Port Description = Alcatel 2/33 6.3.1.636.R01,
Local Slot 2/Port 34 LLDP Info:
Port ID = 2034 (Locally assigned),
Port Description = Alcatel 2/34 6.3.1.636.R01,
Local Slot 2/Port 35 LLDP Info:
Port ID = 2035 (Locally assigned),
Port Description = Alcatel 2/35 6.3.1.636.R01,
Local Slot 2/Port 36 LLDP Info:
Port ID = 2036 (Locally assigned),
Port Description = Alcatel 2/36 6.3.1.636.R01,
Local Slot 2/Port 37 LLDP Info:
Port ID = 2037 (Locally assigned),
Port Description = Alcatel 2/37 6.3.1.636.R01,
Local Slot 2/Port 38 LLDP Info:
Port ID = 2038 (Locally assigned),
Port Description = Alcatel 2/38 6.3.1.636.R01,
Local Slot 2/Port 39 LLDP Info:
Port ID = 2039 (Locally assigned),
Port Description = Alcatel 2/39 6.3.1.636.R01,
Local Slot 2/Port 40 LLDP Info:
Port ID = 2040 (Locally assigned),
Port Description = Alcatel 2/40 6.3.1.636.R01,
Local Slot 2/Port 41 LLDP Info:
Port ID = 2041 (Locally assigned),
Port Description = Alcatel 2/41 6.3.1.636.R01,
Local Slot 2/Port 42 LLDP Info:
Port ID = 2042 (Locally assigned),
Port Description = Alcatel 2/42 6.3.1.636.R01,
```

```

Local Slot 2/Port 43 LLDP Info:
  Port ID                = 2043 (Locally assigned),
  Port Description        = Alcatel 2/43 6.3.1.636.R01,
Local Slot 2/Port 44 LLDP Info:
  Port ID                = 2044 (Locally assigned),
  Port Description        = Alcatel 2/44 6.3.1.636.R01,
Local Slot 2/Port 45 LLDP Info:
  Port ID                = 2045 (Locally assigned),
  Port Description        = Alcatel 2/45 6.3.1.636.R01,
Local Slot 2/Port 46 LLDP Info:
  Port ID                = 2046 (Locally assigned),
  Port Description        = Alcatel 2/46 6.3.1.636.R01,
Local Slot 2/Port 47 LLDP Info:
  Port ID                = 2047 (Locally assigned),
  Port Description        = Alcatel 2/47 6.3.1.636.R01,
Local Slot 2/Port 48 LLDP Info:
  Port ID                = 2048 (Locally assigned),
  Port Description        = Alcatel 2/48 6.3.1.636.R01,

```

output definitions

Port ID	The port ID (Port MAC).
Port Description	The description of the port (which includes the port number and the AOS version).

Release History

Release 7.1.1; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot1	Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

MIB Objects

```

lldpLocPortTable
  lldpLocPortNum
  lldpLocPortIdsubtype
  lldpLocPortId
  lldpLocPortDesc

```

show lldp local-management-address

Displays the local management address information.

```
show lldp local-management-address
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpLocManAddrTable
  lldpLocManAddrLen
  lldpLocManAddrIfSubtype
  lldpLocManAddrIfId
```

show lldp remote-system

Displays per local port and information of remote system.

show lldp [port slot/port [-port] | slot slot] remote-system

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).

slot The slot number for a specific module.

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

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 describes chassis ID.
Chassis ID	The chassis ID (MAC address).
Port ID Subtype	The sub type that describes port ID
Port ID	The port ID (Port MAC).
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.
Capabilites Supported	The capabilities of the system.
Capabilites Enabled	The enabled capabilities of the system.

Release History

Release 7.1.1; 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 config

Displays the general LLDP configuration information for LLDP ports.

show lldp { slot | slot/port [-port]} config

Syntax Definitions

<i>slot</i>	The slot number for a specific module.
<i>slot/port</i>	Slot number for the module and physical port number on that module (e.g., 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 10K, 6900

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

Slot/Port	Admin Status	Notify Trap	Std TLV Mask	Mgmt Address	802.1 TLV	802.3 Mask	MED Mask
2/1	Rx + Tx	Disabled	0x00	Disabled	Disabled	0x00	0x00
2/2	Rx + Tx	Disabled	0x00	Disabled	Disabled	0x00	0x00
2/3	Rx + Tx	Disabled	0x00	Disabled	Disabled	0x00	0x00
2/4	Rx + Tx	Disabled	0x00	Disabled	Disabled	0x00	0x00
2/5	Rx + Tx	Disabled	0x00	Disabled	Disabled	0x00	0x00

output definitions

Slot/Port	Specifies the LLDP slot and port number.
Admin Status	Specifies the Administrative status of the LLDP port. The options are - Disabled, Rx, Tx, and Rx+Tx.
Notify Trap	Specifies if the Notify Trap feature is disabled or enabled on a particular port
Std TLV Mask	Specifies the standard TLV mask set for the port.
Mgmt Address	Specifies whether transmission of the per port IPv4 management address is enabled or disabled.
802.1 TLV	Specifies whether 802.1 TLV status is enabled or disabled on the LLDP port.

output definitions

802.3 Mask	Specifies the standard 802.3 mask set for the port.
MED Mask	Specifies the standard MED mask set for the port.

Release History

Release 7.1.1; command introduced.

Related Commands

lldp lldpdu	Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
lldp notification	Specifies the switch to control per port notification status about the remote device change.
lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot3	Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.

MIB Objects

```
lldpPortConfigTable
  lldpPortConfigPortNum
  lldpPortConfigAdminStatus
  lldpPortConfigNotificationEnable
  lldpLocPortPortNum
  lldpPortConfigTLVsTxEnable
lldpConfigManAddrTable
  lldpConfigManAddrPortsTxEnable
lldpXdot3PortConfigTable
  lldpXdot3PortConfigTLVsTxEnable
```

show lldp statistics

Displays per port statistics.

show lldp [port slot/port [-port] slot slot] statistics

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).

slot The slot number for a specific module.

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the slot/port option is not specified, statistics for the chassis is displayed.
- If the statistics are zero they are not displayed.

Examples

```
-> show lldp statistics
```

Slot/Port	Tx	LLDPDU Rx	Errors	Discards	TLV Unknown	Device 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 7.1.1; command introduced.

Related Commands

lldp lldpdu

Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

lldp tlv management

Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

MIB Objects

lldpStatsTxPortTable

 lldpStatsTxPortNum

 lldpStatsTxPortFramesTotal

lldpStatsRxPortTable

 lldpStatsRxPortNum

 lldpStatsRxPortFramesDiscardedTotal

 lldpStatsRxPortFramesErrors

 lldpStatsRxPortFramesTotal

 lldpStatsRxPortTLVsDiscardedTotal

 lldpStatsRxPortTLVsUnrecognizedTotal

 lldpStatsRxPortAgeoutsTotal

show lldp remote-system med

Displays remote system MED information for a single port or all ports on a slot.

show lldp [*slot/port* [-*port*] | *slot*] **remote-system** [**med** {**network-policy** | **inventory**}]

Syntax Definitions

<i>slot/port</i>	Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>slot</i>	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 10K, 6900

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  Untagge 345     4         34
1/22   2           Guest Voice(4) Defined  Untagge 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 7.1.1; 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
```

13 IP Commands

This chapter details Internet Protocol (IP) commands for the switch. IP is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be forwarded. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols.

IP is enabled on the switch by default and there are few options that can, or need to be, configured. This chapter provides instructions for basic IP configuration commands. It also includes commands for several Layer 3 and Layer 4 protocols that are associated with IP:

- Address Resolution Protocol (ARP)—Used to match the IP address of a device with its physical (MAC) address.
- Internet Control Message Protocol (ICMP)—Specifies the generation of error messages, test packets, and informational messages related to IP. ICMP supports the [ping](#) command that is used to determine if hosts are online.
- Transmission Control Protocol (TCP)—A major data transport mechanism that provides reliable, connection-oriented, full-duplex data streams. While the role of TCP is to add reliability to IP, TCP relies upon IP to do the actual delivering of datagrams.
- User Datagram Protocol (UDP)—A secondary transport-layer protocol that uses IP for delivery. UDP is not connection-oriented and does not provide reliable end-to-end delivery of datagrams. But some applications can safely use UDP to send datagrams that do not require the extra overhead added by TCP.

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. If all devices are on the same VLAN or if the IP interfaces are created on multiple VLANs to enable routing of packets, packets can be forwarded using IP. However, IP routing requires one of the IP routing protocols: Routing Information Protocol (RIP) or Open Shortest Path First (OSPF). See the following chapters for the appropriate CLI commands: [Chapter 16, “RIP Commands,”](#) [Chapter 20, “OSPF Commands.”](#) For more information on VLANs and RIP, see the applicable chapters in the Configuration Guide. For more information on OSPF, see the “Configuring OSPF” chapter in the *OmniSwitch AOS Release 7 Advanced Routing Configuration Guide*.

MIB information for the IP commands is as follows:

Filename: IpForward.mib
Module: IpForward

Filename: Ip.mib
Module: Ip

Filename: AlcatelIND1Ip.mib
Module: alcatelIND1IPMIB

Filename: AlcatelIND1Iprm.mib
Module: alcatelIND1IPRMMIB

A summary of the available commands is listed here:

IP	<code>ip interface</code> <code>ip interface tunnel</code> <code>ip router primary-address</code> <code>ip router router-id</code> <code>ip static-route</code> <code>ip route-pref</code> <code>ip default-ttl</code> <code>ping</code> <code>traceroute</code> <code>ip directed-broadcast</code> <code>ip service</code> <code>ip service port</code> <code>show ip traffic</code> <code>show ip interface</code> <code>show ip routes</code> <code>show ip route-pref</code> <code>show ip redistrib</code> <code>show ip access-list</code> <code>show ip route-map</code> <code>show ip router database</code> <code>show ip emp-routes</code> <code>show ip config</code> <code>show ip protocols</code> <code>show ip router-id</code> <code>show ip service</code>
IP Route Map Redistribution	<code>ip redistrib</code> <code>ip access-list</code> <code>ip access-list address</code> <code>ip route-map action</code> <code>ip route-map match ip address</code> <code>ip route-map match ipv6 address</code> <code>ip route-map match ip-nexthop</code> <code>ip route-map match ipv6-nexthop</code> <code>ip route-map match tag</code> <code>ip route-map match ipv4-interface</code> <code>ip route-map match ipv6-interface</code> <code>ip route-map match metric</code> <code>ip route-map match route-type</code> <code>ip route-map match protocol</code> <code>ip route-map set metric</code> <code>ip route-map set metric-type</code> <code>ip route-map set tag</code> <code>ip route-map set community</code> <code>ip route-map set local-preference</code> <code>ip route-map set level</code> <code>ip route-map set ip-nexthop</code> <code>ip route-map set ipv6-nexthop</code> <code>show ip redistrib</code> <code>show ip access-list</code> <code>show ip route-map</code>
Multiple Virtual Routing and Forwarding (VRF)	<code>vrf</code> <code>show vrf</code>
Virtual Routing and Forwarding - Route Leak	<code>ip export route-map</code> <code>ip import vrf</code> <code>show ip export</code> <code>show ip import</code> <code>show ip global-route-table</code>

ARP	arp clear arp-cache ip dos arp-poison restricted-address arp filter clear arp filter show arp show ip dos arp-poison show arp filter
ICMP	icmp type icmp unreachable icmp echo icmp timestamp icmp addr-mask icmp messages show icmp control show icmp statistics
TCP	show tcp statistics show tcp ports
UDP	show udp statistics show udp ports
Denial of Service (DoS)	ip dos scan close-port-penalty ip dos scan tcp open-port-penalty ip dos scan udp open-port-penalty ip dos scan threshold ip dos trap ip dos scan decay show ip dos config show ip dos statistics

ip interface

Configures an IP interface to enable IP routing on a VLAN or allow remote access. Without an IP interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

ip interface {*name* | **emp**} [{**address** | **vip-address**} *ip_address*] [**mask** *subnet_mask*] [**admin-state** [**enable** | **disable**]] [**vlan** *vlan_id*] [**forward** | **no forward**] [**local-proxy-arp** | **no local-proxy-arp**] [**e2** | **snap**] [**primary** | **no primary**]

no ip interface *name*

Syntax Definitions

<i>name</i>	Text string of interface name. Use quotes around string if description contains multiple words with spaces between them (for example, “Alcatel-Lucent Marketing”). This value is case sensitive.
emp	Modifies the shared EMP port IP address.
address <i>ip_address</i>	An IP host address (for example, 10.0.0.1, 171.15.0.20) to specify the IP router network.
vip-address <i>ip_address</i>	An IP host address for a Virtual IP (VIP) VLAN. This type of IP address is used only in a Multi-Chassis Link Aggregation (MC-LAG) configuration.
<i>subnet_mask</i>	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.
<i>vlan_id</i>	An existing VLAN ID number (1–4094). Specify a multi-chassis VLAN ID if the IP interface is for a VIP VLAN.
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.
e2	Enter e2 or ethernet2 to specify 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.

Defaults

parameter	default
<i>ip_address</i>	0.0.0.0
<i>subnet_mask</i>	IP address class
enable disable	enable
<i>vlan_id</i>	none (unbound)
forward no forward	forward
local-proxy-arp no local-proxy-arp	no local-proxy-arp
e2 snap	e2
primary no primary	First interface bound to a VLAN.

Platforms Supported

OmniSwitch 10K, 6900

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 16 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.
- To configure a virtual IP interface for an MC-LAG VLAN (VIP VLAN), use the **vip-address** parameter and specify a multi-chassis VLAN ID for the interface **vlan** parameter.
- When local proxy ARP is enabled for any one IP router interface associated with a VLAN, the feature is applied to the entire VLAN. It is not necessary to enable it for each interface. However, if the IP interface that has this feature enabled is moved to another VLAN, Local Proxy ARP is enabled for the new VLAN and must be enabled on another interface for the old VLAN.
- When Local Proxy ARP is enabled, all traffic is routed instead of bridged within the VLAN. ARP requests return the MAC address of the IP router interface. The same MAC address is assigned to each interface configured for a VLAN.
- Local Proxy ARP takes precedence over any switch-wide ARP or Proxy ARP function. It is not necessary to have Proxy ARP configured to use Local Proxy ARP. The two features are independent of each other.
- By default, the first interface bound to a VLAN becomes the primary interface for that VLAN. Use the **primary** keyword with this command to configure a different IP interface as the primary.
- To create an IP interface for network management purposes, specify **Loopback0** (case sensitive) as the name of the interface. The Loopback0 interface is not bound to any VLAN, so it always remains operationally active.

Examples

```
-> ip interface "Marketing"
-> ip interface "Payroll address" 18.12.6.3 vlan 255
```

```
-> ip interface "Human Resources" 10.200.12.101 vlan 500 no forward snap
-> ip interface "Distribution" 11.255.14.102 vlan 500 local-proxy-arp primary
```

Release History

Release 7.1.1; command introduced

Related Commands

[show ip interface](#) Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable
  alaIpInterfaceName
  alaIpInterfaceAddress
  alaIpInterfaceVipAddress
  alaIpInterfaceMask
  alaIpInterfaceAdminState
  alaIpInterfaceDeviceType
  alaIpInterfaceVlanID
  alaIpInterfaceIpForward
  alaIpInterfaceEncap
  alaIpInterfaceLocalProxyArp
  alaIpInterfacePrimCfg
  alaIpInterfaceOperState
  alaIpInterfaceOperReason
  alaIpInterfaceRouterMac
  alaIpInterfaceBcastAddr
  alaIpInterfacePrimAct
```

ip interface tunnel

Configures the end points for a GRE or IPIP tunnel.

ip interface *name* **tunnel** [**source** *ip_address*] [**destination** *ip_address*] [**protocol** {**ipip** | **gre**}]

Syntax Definitions

<i>name</i>	Text string. Use quotes around string if description contains multiple words with spaces between them (for example, "Alcatel-Lucent Marketing"). This value is case sensitive.
source <i>ip_address</i>	Source IP address of the tunnel.
destination <i>ip_address</i>	Destination IP address of the tunnel.
ipip	Specifies the tunneling protocol as IPIP.
gre	Specifies the tunneling protocol as GRE.

Defaults

parameter	default
ipip gre	ipip

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

You can configure an interface as either a VLAN or tunnel interface.

Examples

```
-> ip interface "tnl-1" tunnel source 23.23.23.1 destination 155.2.2.2 protocol gre
-> ip interface "tnl-1" tunnel source 23.23.23.1 destination 155.2.2.2 protocol
ipip
```

Release History

Release 7.1.1; command introduced

Related Commands

[show ip interface](#) Displays the status and configuration of IP interfaces.

MIB Objects

```
alaIpInterfaceTable  
  alaIpInterfaceName  
  alaIpInterfaceTunnelSrc  
  alaIpInterfaceTunnelDst  
  alaIpInterfaceDeviceType
```

ip router primary-address

Configures the router primary IP address. By default, the router primary address is derived from the first IP interface that becomes operational on the router.

ip router primary-address *ip_address*

Syntax Definitions

ip_address 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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.

Examples

```
-> ip router primary-address 172.22.2.115
```

Release History

Release 7.1.1; 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 10K, 6900

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.
- The router ID is used by OSPF and BGP for unique identification of the router in the network.

Examples

```
-> ip router router-id 172.22.2.115
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip router primary-address](#) Configures the router primary IP address.

MIB Objects

alaDcrTmConfig
 alaDrcTmIpRouterId

ip static-route

Creates/deletes an IP static route. 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*/**follows** *ip_address* [**metric** *metric*]

no ip static-route *ip_address* [**mask** *mask*] **gateway** *ip_address*/**follows** *ip_address* [**metric** *metric*]

Syntax Definitions

<i>ip_address</i>	Destination IP address of the static route.
<i>mask</i>	Subnet mask corresponding to the destination IP address.
gateway <i>ip_address</i>	IP address of the next hop used to reach the destination IP address.
follows <i>ip_address</i>	The recursive static route follows this IP address. The recursive route uses the same gateway or nexthop that is used to reach this host address.
<i>metric</i>	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
<i>metric</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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**.

Examples

```
-> ip static-route 171.11.1.1 gateway 171.11.2.1
-> ip static-route 0.0.0.0 mask 0.0.0.0 gateway 171.11.2.1
-> ip static-route 171.11.0.0 follows 192.168.10.1
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip routes	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.

[vrf name] ip route-pref {static | rip | ospf | isisl2 | isisl1 | ibgp | ebgp | import} value

Syntax Definitions

<i>name</i>	The alphanumeric name (1–20 characters) assigned to the VRF instance.
static	Configures the route preference of static routes.
ospf	Configures the route preference of OSPF routes.
isisl2	Configures the route preference of ISIS L2 routes.
isisl1	Configures the route preference of ISIS L1 routes.
rip	Configures the route preference of RIP routes.
ebgp	Configures the route preference of external BGP routes.
ibgp	Configures the route preference of internal BGP routes.
import	Configures the route preference for the routes that are imported.
<i>value</i>	Route preference value.

Defaults

parameter	default
static value	2
ospf value	110
isisl2 value	118
isisl1 value	115
rip value	120
ebgp value	190
ibgp value	200
import value	210

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Route preference of local routes cannot be changed.

Examples

```
-> ip route-pref ebgp 20
-> ip route-pref rip 60
-> ip route-pref import 210
```

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** and **import** parameters added.

Related Commands

show ip route-pref	Displays the configured route-preference of a router.
ip import vrf	Configures a route map to import routes from GRT to the destination VRF.
show ip import	Displays the import route configuration details.

MIB Objects

```
alaIprmRtPrefTable
  alaIprmRtPrefEntryType
  alaIprmRtPrefEntryValue
```

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 travels before being discarded.

ip default-ttl *hops*

Syntax Definitions

hops TTL value, in hops. Valid range is 1–255.

Defaults

parameter	default
<i>hops</i>	64

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced

Related Commands

[show ip config](#) Displays IP configuration parameters.

MIB Objects

IpDefaultTTL

ping

Tests whether an IP destination can be reached from the local switch. This command sends an ICMP echo request to a destination and then waits for a reply. To ping a destination, enter the **ping** command and enter either the IP address or hostname of the destination. 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 below.

ping {*ip_address* / *hostname*} [**source-interface** *ip_interface*] [**count** *count*] [**size** *packet_size*] [**interval** *seconds*] [**timeout** *seconds*] [**data-pattern** *string*] [**dont-fragment**] [**tos** *tos_val*]

Syntax Definitions

<i>ip_address</i>	IPv4 address of the system to ping.
<i>hostname</i>	DNS name of the system to ping.
<i>count</i>	Number of frames to be transmitted.
<i>packet_size</i>	Size of the data portion of the packet sent for this ping, in bytes. Valid range is 1–65507.
interval <i>seconds</i>	Polling interval. The switch polls the host at time intervals specified in seconds.
timeout <i>seconds</i>	Number of seconds the program waits for a response before timing out.
source-interface <i>ip_interface</i>	IP address to be used as source IP for the ping packets.
data-pattern <i>string</i>	The data pattern to be used in the data field of the ping packets.
dont-fragment	Sets the don't-fragment bit in the IP packet.
tos <i>tos_val</i>	Type of Service field in the IP header.

Defaults

parameter	default
<i>count</i>	6
<i>packet_size</i>	64
interval <i>seconds</i>	1
timeout <i>seconds</i>	5
dont-fragment	0
tos <i>tos_val</i>	0
data-pattern <i>string</i>	Repeating sequence of ASCII characters 0x4 onwards to 0xff

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you change the default values, they are only applied to the current ping. The next time you use the ping command, the default values are used unless you again enter different values.

Examples

```
-> ping 10.255.11.242

PING 10.255.11.242: 56 data bytes
64 bytes from 10.255.11.242: icmp_seq=0. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=1. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=2. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=3. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=4. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=5. time=0. ms
----10.255.11.242 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0

-> ping 10.0.0.1 source-interface mgmt
-> ping 10.0.0.1 tos 1
-> ping 10.0.0.1 timeout 10
-> ping 10.0.0.1 interval 10
-> ping 10.0.0.1 dont-fragment
-> ping 10.0.0.1 data-pattern AB
```

Release History

Release 7.1.1; command introduced

Related Commands

traceroute Finds the path taken by an IP packet from the local switch to a specified destination.

traceroute

Finds the path taken by an IP packet from the local switch to a specified destination. This command displays the individual hops to the destination as well as some timing information.

traceroute {*ip_address* / *hostname*} [**max-hop** *max_hop_count*] [**min-hop** *min_hop_count*] [**source-interface** *ip_interface*] [**probes** *probe_count*] [**timeout** *seconds*] [**port** *port_number_value*]

Syntax Definitions

<i>ip_address</i>	IPv4 address of the host whose route you want to trace.
<i>hostname</i>	DNS name of the host whose route you want to trace.
<i>max_hop_count</i>	Maximum hop count for the trace. The valid range is 1–255.
<i>min_hop_count</i>	Minimum hop count for the trace. The valid range is 1–30.
source-interface <i>ip_interface</i>	Source IP interface to be used in the traceroute packets.
probes <i>probe_count</i>	The number of packets (retry) sent for each hop-count. The valid range is 1–10000.
timeout <i>seconds</i>	The time to wait for the response of each probe packet.
port <i>port_number_value</i>	The destination port number to be used in the probing packets.

Defaults

parameter	default
max-hop <i>max_hop_count</i>	30
min-hop <i>min_hop_count</i>	1
source-interface <i>ip_interface</i>	Outgoing IP interface as per route lookup
probes <i>probe_count</i>	3
timeout <i>seconds</i>	5
port <i>port_number_value</i>	33334

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When using this command, you must enter the name of the destination as part of the command line (either the IP address or host name).

Examples

```
-> traceroute 128.251.17.224

traceroute to 128.251.17.224, 30 hops max, 40 byte packets
 1 10.255.11.254 0 ms 0 ms 0 ms
 2 172.23.0.251 0 ms 16.6667 ms 0 ms
 3 128.251.14.253 0 ms 0 ms 0 ms
 4 128.251.17.224 0 ms 0 ms 0 ms

-> traceroute 128.251.17.224 max-hop 3
traceroute to 128.251.17.224, 3 hops max, 40 byte packets
 1 10.255.11.254 0 ms 0 ms 0 ms
 2 172.23.0.251 16.6667 ms 0 ms 0 ms
 3 128.251.14.253 0 ms 0 ms 0 ms
-> traceroute 10.0.0.1 source-interface mgmt
-> traceroute 10.0.0.1 min-hop 3
-> traceroute 10.0.0.1 probes 3
-> traceroute 10.0.0.1 timeout 10
-> traceroute 10.0.0.1 port-number 1025
```

Release History

Release 7.1.1; command introduced

Related Commands

[show ip routes](#) Displays the IP Forwarding table.

MIB Objects

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 zeros or all 1s in the host portion of the destination address. The packet is sent to the broadcast address of a subnet to which the sender is not directly attached.

ip directed-broadcast {on | off}

Syntax Definitions

N/A

Defaults

The default value is **off**.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Directed broadcasts are used in denial-of-service “smurf” attacks. In a smurf attack, a continuous stream of ping requests are sent from a falsified source address to a directed broadcast address. This results in a large stream of replies, which can overload the host of the source address. By default, the switch drops directed broadcasts. Directed broadcasts must not be enabled.

Examples

```
-> ip directed-broadcast off
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip interface	Displays the status and configuration of IP interfaces.
show ip routes	Displays the IP Forwarding table.
show ip config	Displays IP configuration parameters.

MIB Objects

```
alaIpDirectedBroadcast
```

ip service

Enables (opens) or disables (closes) well-known or user-defined TCP/UDP service ports. Selectively enabling or disabling these types of ports provides an additional method for protecting against unauthorized switch access or Denial of Service (DoS) attacks.

```
[vrf name] ip service {all | service_name | port service_port} admin-state {enable | disable}
```

Syntax Definitions

<i>name</i>	Specifies the name of the VRF in which services are to be enabled or disabled.
all	Configures access to all TCP/UDP ports.
<i>service_name</i>	The name of the TCP/UDP service to enable or disable. (Refer to the table in the “Usage Guidelines” section for a list of supported service names.)
<i>service_port</i>	A TCP/UDP service port number. Configures access by port number rather than by service name. (Refer to the table in the “Usage Guidelines” section for a list of well-known port numbers.) If a user-defined port number is specified, the valid range is 20000–20999.
enable	Enables access to the service.
disable	Disables access to the service.

Defaults

All TCP/UDP ports are open by default.

Platforms Supported

OmniSwitch 10K, 6900

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 “Example” section for more information.
- When specifying a service port number, the **port** keyword is required and that only one port number is allowed in a single command.

- The following table lists the **ip service** command options for specifying TCP/UDP services and also includes the well-known port number associated with each service:

service name	port
ftp	21
ssh	22
telnet	23
http	80
https	443
ntp	123
snmp	161

- If a VRF is specified, the service is enabled or disabled in the specified VRF. By default, the services are enabled in the 'default' VRF.

Examples

```
-> ip service all admin-state disable
-> ip service ftp admin-state enable
-> ip service port 20000 admin-state enable
-> vrf vrfl ip service ftp admin-state enable
```

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** parameter added.

Related Commands

ip service port Configures a user-defined TCP/UDP port for the specified service.
show ip service Displays the IP service TCP/UDP port configuration and status.

MIB Objects

```
alaIpServiceTable
  alaIpServiceType
  alaIpServicePort
  alaIpServiceStatus
alaIpPortServiceTable
  alaIpPortServicePort
  alaIpPortServiceStatus
```

ip service port

Configures a user-defined TCP/UDP service port for the specified service.

ip service {*service_name*} **port** {**default** | *service_port*}

Syntax Definitions

<i>service_name</i>	The name of the TCP/UDP service to enable or disable. (Refer to the table in the “Usage Guidelines” section for a list of supported service names.)
<i>service_port</i>	A TCP/UDP service port number (Refer to the table in the “Usage Guidelines” section for a list of supported service names.) Valid range is the default service port number or 20000-20999.
default	Sets the port back to the well-known port for the specified service.

Defaults

By default, the service uses the well-known TCP/UDP port number for that service.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **default** parameter with this command to set the port for the specified service back to the well-known default port for that service. For example, if the FTP port was previously changed to “20000”, then the **ip service ftp port default** command would set the FTP port back to “21”.
- The following table lists the **ip service port** command options for specifying TCP/UDP services and also includes the default well-known port number associated with each service:

service name	port
ftp	21
ssh	22
telnet	23
http	80
https	443

ntp and **snmp** services are not supported with the **ip service port** command.

- Use the **ip service** command to enable or disable the status for a well-known or user-defined TCP/UDP service port.

Examples

```
-> ip service ftp port 20000
-> ip service ftp port default
```



```
-> ip service telnet port 20003
-> ip service telnet port default
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip service](#)

Enables or disables well-known or user-defined service ports.

[show ip service](#)

Displays the IP service TCP/UDP port configuration and status.

MIB Objects

```
alaIpServiceTable
  alaIpServiceType
  alaIpServicePort
  alaIpServiceStatus
```

ip redist

Controls the conditions for redistributing IPv4 routes between different protocols.

```
[vrf name] ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} route-map
route-map-name [status {enable | disable}]
```

```
no ip redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} [route-map
route-map-name]
```

Syntax Definitions

local	Redistributes local routes.
static	Redistributes static routes.
import	Redistributes routes to other routing protocols that are imported.
rip	Specifies RIP as the source or destination (into) protocol.
ospf	Specifies OSPF as the source or destination (into) protocol.
isis	Specifies IS-IS as the source or destination (into) protocol.
bgp	Specifies BGP as the source or destination (into) protocol.
<i>route-map-name</i>	Name of an existing route map that controls 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 10K, 6900

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 7 Network Configuration Guide* for more information about how to create a route map.

Examples

```
-> ip redistrib rip into bgp route-map rip-to-bgp1
-> ip redistrib rip into bgp route-map rip-to-bgp2
-> no ip redistrib rip into bgp route-map rip-to-bgp2
-> ip redistrib ospf into rip route-map ospf-to-rip
-> ip redistrib ospf into rip route-map ospf-to-rip disable
-> ip redistrib import into ospf route-map R1 status enable
```

Release History

Release 7.1.1; command introduced

Release 7.3.1; **vrf** and **import** parameters added.

Related Commands

show ip redistrib	Displays the route map redistribution configuration.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip import vrf	Configures a route map to import routes from GRT to the destination VRF.
show ip import	Displays the import route configuration details.

MIB Objects

```
alaRouteMapRedistProtoTable
  alaRouteMapRedistSrcProtoId
  alaRouteMapRedistDestProtoId
  alaRouteMapRedistRouteMapIndex
  alaRouteMapRedistStatus
  alaRouteMapRedistAddressType
  alaRouteMapRedistRowStatus
```

ip access-list

Creates an access list for adding multiple IPv4 addresses to route maps.

ip access-list *access-list-name*

no ip access-list *access-list-name*

Syntax Definitions

access-list-name Name of the access list (up to 20 characters).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>access-list-name</i>	Name of the access list.
<i>address/prefixLen</i>	IP address/prefix length to be added to the access list.
permit	Permits the IP address.
deny	Denies the IP address.
all-subnets	Permits or denies all the subnet routes that match the network portion of the IP address as specified by the mask length
no-subnets	Permits or denies only those routes that exactly match the IP address and the mask length.
aggregate	Permits an aggregate route if there are one or more routes that match or are subnets of this address.

Defaults

parameter	default
permit deny	permit
all-subnets no-subnets aggregate	all-subnets

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 the 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.
- The **redist-control** parameters (**all-subnets**, **no-subnets**, and **aggregate**) defines the criteria used to determine if a route matches an address in the access list.
- Configuring the combination of **redist-control aggregate** with **action deny** is not allowed.
- Use this command multiple times with the same access list name to add multiple addresses to the existing access list.

Examples

```
-> ip access-list access1 address 10.0.0.0/8 action permit
-> ip access-list access1 address 11.1.0.0/16 action permit
-> ip access-list access1 address 10.1.1.0/24 redist-control aggregate
-> no ip access-list access1 address 10.0.0.0/8
```

Release History

Release 7.1.1; command introduced

Related Commands

ip access-list	Creates an access list for adding multiple IPv4 addresses to route maps.
show ip access-list	Displays the contents of an IPv4 access list.

MIB Objects

```
alaRouteMapAccessListTable
  alaRouteMapAccessListIndex
  alaRouteMapAccessListAddress
  alaRouteMapAccessListAddressType
  alaRouteMapAccessListPrefixLength
  alaRouteMapAccessListAction
  alaRouteMapAccessListRedistControl
  alaRouteMapAccessListRowStatus
```

ip route-map action

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

ip route-map *route-map-name* [**sequence-number** *number*] **action** {**permit** | **deny**}

no ip route-map *route-map-name* [**sequence-number** *number*]

Syntax Definitions

<i>route-map-name</i>	The name of the route map (up to 20 characters).
<i>number</i>	A number that links together the route maps. The range is 1–100.
permit	Selects a route.
deny	Filters a route.

Defaults

parameter	default
<i>number</i>	50
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

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 routel sequence-number 10 action permit
-> no ip route-map routel
```

Release History

Release 7.1.1; 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

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>access-list-name</i>	The name of an IPv4 access list that contains IPv4 addresses to match.
<i>ip_address/prefixLen</i>	The destination IP address along with the prefix length of the routes to be selected.
all-subnets	Selects all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Selects only those routes that exactly match the IP address and the mask length.
aggregate	Creates an aggregate route if there are one or more routes that match the IP address.
permit	Permits a route based on the IP address or prefix constrained by redist-control.
deny	Denies a route based on the IP address or prefix constrained by redist-control.

Defaults

parameter	default
<i>number</i>	50
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **match ip-address redist-control** parameter in the route map.
- Specify either the name of an existing IPv4 access list or an IPv4 address/prefix length with this command.

- Configuring the combination of **redist-control aggregate** with **deny** is not allowed.
- Multiple addresses in the same route map sequence are matched using the longest prefix match.
- If the best matching address is type **deny**, then the route is not selected. If the best matching address is type **permit** and the route map action is **deny**, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name*, **sequence-number**, and *access-list-name* (if used) must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 3 match ip-address 10.1.1.1/8 redist-control no-subnets deny
-> no ip route-map 3 match ip-address 10.1.1.1 redist-control no-subnets deny
-> ip route-map routel sequence-number 10 match ip-address list1
-> no ip route-map routel sequence-number 10 match ip-address list1
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip 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

<i>route-map-name</i>	The name of the route map (up to 20 characters).
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>access-list-name</i>	The name of an IPv4 access list that contains IPv4 addresses to match.
<i>ipv6_address/prefixLen</i>	The destination IPv6 address along with the prefix length of the routes to be selected.
all-subnets	Selects all the subnet routes that match the network portion of the IP address as specified by the mask length.
no-subnets	Selects only those routes that exactly match the IP address and the mask length.
aggregate	Creates an aggregate route if there are one or more routes that match the IPv6 address.
permit	Permits a route based on the IPv6 address or prefix constrained by redist-control .
deny	Denies a route based on the IPv6 address or prefix constrained by redist-control .

Defaults

parameter	default
<i>number</i>	50
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv6-address redist-control** parameter in the route map.
- Specify either the name of an existing IPv6 access list or an IPv6 address/prefix length with this command.

- Configuring the combination of **redist-control aggregate** with **deny** is not allowed.
- Multiple addresses in the same route map sequence are matched using the longest prefix match.
- If the best matching address is type **deny**, then the route is not selected. If the best matching address is type **permit** and the route map action is **deny**, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 3 match ipv6-address 2001::1/64 redist-control no-subnets deny
-> no ip route-map 3 match ipv6-address 2001::1/64 redist-control no-subnets deny
-> ip route-map route1 sequence-number 10 match ipv6-address list1
-> no ip route-map route1 sequence-number 10 match ipv6-address list1
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[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-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**]}

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>access-list-name</i>	The access list that matches the route nexthop IP address.
<i>ip_address/prefixLen</i>	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
<i>number</i>	50
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **match ip-nexthop** parameter in the route map.
- If the best matching nexthop is type **deny**, then the route is not selected. If the best matching nexthop is type **permit** and the route map action is **deny**, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name*, **sequence-number**, and *access-list-name* must exist before you configure this **match** criteria.

Examples

```
-> ip route-map routel sequence-number 10 match ip-nexthop list1
-> no ip route-map routel sequence-number 10 match ip-nexthop list1
-> ip route-map routel sequence-number 10 match ip-nexthop 10.0.0.0/8
-> no ip route-map routel sequence-number 10 match ip-nexthop 10.0.0.0/8
```

Release History

Release 7.1.1; 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 selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[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

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>access-list-name</i>	The access list that matches the route nexthop IPv6 address.
<i>ipv6_address/prefixLen</i>	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
<i>number</i>	50
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **match ipv6-nexthop** parameter in the route map.
- If the best matching nexthop is type **deny**, then the route is not selected. If the best matching nexthop is type **permit** but the route map action is **deny**, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name*, **sequence-number**, and *access-list-name* must exist before you configure this **match** criteria.

Examples

```
-> ip route-map routel sequence-number 10 match ipv6-nexthop list1
-> no ip route-map routel sequence-number 10 match ipv6-nexthop list1
-> ip route-map routel sequence-number 10 match ipv6-nexthop 2001::/64
-> no ip route-map routel sequence-number 10 match ipv6-nexthop 2001::/64
```

Release History

Release 7.1.1; 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 selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
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

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>tag-number</i>	The tag number.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

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 routel sequence-number 10 match tag 4
-> no ip route-map routel sequence-number 10 match tag 4
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
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

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>interface-name</i>	Specifies the interface name of the outgoing interface of the route.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

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 routel sequence-number 10 match ipv4-interface int4  
-> no ip route-map routel sequence-number 10 match ipv4-interface int4
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

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

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>interface-name</i>	Specifies the interface name of the outgoing interface of the route.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

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 routel sequence-number 10 match ipv6-interface int6
-> no ip route-map routel sequence-number 10 match ipv6-interface int6
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

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

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>metric</i>	The metric value that matches a specified metric.
<i>deviation</i>	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
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

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 routel sequence-number 10 match metric 4
-> no ip route-map routel sequence-number 10 match metric 4
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[show ip route-map](#)

Displays the configured IP route maps.

MIB Objects

alaRouteMapTable

alaRouteMapIndex

alaRouteMapSequence

alaRouteMapType

alaRouteMapValue

alaRouteMapRowStatus

ip route-map match route-type

Matches the specified route type with actual route type of the route.

ip route-map *route-map-name* [**sequence-number** *number*] **match route-type** {**internal** | **external** [**type1** | **type2**] | **level1** | **level2**}

no ip route-map *route-map-name* [**sequence-number** *number*] **match route-type** {**internal** | **external** [**type1** | **type2**] | **level1** | **level2**}

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
internal	Matches OSPF/BGP internal routes.
external	Matches OSPF/BGP external routes.
type1	Matches OSPF external Type-1 routes, which gives the full metric calculation for the complete path including internal as well as external cost.
type2	Matches OSPF external Type-2 routes, which gives the external redistribution metric only to the ASBR.
level1	Matches IS-IS Level-1 routes only.
level2	Matches IS-IS Level-2 routes only.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **match route-type** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 match route-type internal
-> no ip route-map 111 sequence-number 50 match route-type internal
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[show ip route-map](#)

Displays the configured IP route maps.

MIB Objects

```
alaRouteMapTable
  alaRouteMapIndex
  alaRouteMapSequence
  alaRouteMapType
  alaRouteMapValue
  alaRouteMapRowStatus
```

ip route-map match protocol

Matches the protocol specified in the route map with the protocol of the route.

ip route-map *route-map-name* [**sequence-number** *number*] **match protocol** {**local** | **static** | **rip** | **ospf** | **isis** | **bgp**}

no ip route-map *route-map-name* [**sequence-number** *number*] **match protocol** {**local** | **static** | **rip** | **ospf** | **isis** | **bgp**}

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
local	Matches a local interface route.
static	Matches a static route.
rip	Matches a RIP route.
ospf	Matches an OSPF route.
ISIS	Matches an ISIS route.
bgp	Matches a BGP route.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **match protocol** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **match** criteria.

Examples

```
-> ip route-map routel sequence-number 10 match protocol local
-> no ip route-map routel sequence-number 10 match protocol local
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[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

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>metric</i>	Configures the metric value of the route. A value of 0 is not allowed.
add	Adds the configured metric value to the actual metric value.
subtract	Subtracts the configured metric value from the actual metric value.
replace	Replaces the actual metric value with the configured metric value.
none	Uses the actual metric value of the route. The configured metric value is ignored. Use any value except 0.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[show ip route-map](#)

Displays the configured IP route maps.

MIB Objects

alaRouteMapTable

alaRouteMapIndex

alaRouteMapSequence

alaRouteMapType

alaRouteMapValue

alaRouteMapRowStatus

ip route-map set metric-type

Configures the metric type for the redistributed route.

```
ip route-map route-map-name [sequence-number number] set metric-type
{internal | external [type1 | type2]}
```

```
no ip route-map route-map-name [sequence-number number] set metric-type
{internal | external [type1 | type2]}
```

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
internal	Sets the metric type to internal for routes redistributed into BGP.
external	Sets the metric type to external for routes redistributed into BGP.
type1	Sets the metric type to external type1 for routes redistributed into OSPF, which gives the full metric calculation for the complete path including internal as well as external cost.
type2	Sets the metric type to external type2 for routes redistributed into OSPF, which gives the external redistribution metric only to the ASBR.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **set metric-type** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set metric-type internal
-> no ip route-map 111 sequence-number 50 set metric-type internal
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[show ip route-map](#)

Displays the configured IP route maps.

MIB Objects

alaRouteMapTable

alaRouteMapIndex

alaRouteMapSequence

alaRouteMapType

alaRouteMapValue

alaRouteMapRowStatus

ip route-map set tag

Configures the tag value of the selected routes.

```
ip route-map route-map-name [sequence-number number] set tag tag-number
```

```
no ip route-map route-map-name [sequence-number number] set tag tag-number
```

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>tag-number</i>	Configures the tag number.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

alaRouteMapTable

 alaRouteMapIndex

 alaRouteMapSequence

 alaRouteMapType

 alaRouteMapValue

 alaRouteMapRowStatus

ip route-map set community

Configures the community name of the route being redistributed into BGP.

ip route-map *route-map-name* [**sequence-number** *number*] **set community** *community-string*

no ip route-map *route-map-name* [**sequence-number** *number*] **set community** *community-string*

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>community-string</i>	Defines a community for an aggregate route. Community names range from 0 to 70 characters.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **set community** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set community 29
-> no ip route-map 111 sequence-number 50 set community 29
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
show ip route-map	Displays the configured IP route maps.

MIB Objects

alaRouteMapTable

 alaRouteMapIndex

 alaRouteMapSequence

 alaRouteMapType

 alaRouteMapValue

 alaRouteMapRowStatus

ip route-map set local-preference

Configures the local preference value for a route being distributed into BGP.

ip route-map *route-map-name* [**sequence-number** *number*] **set local-preference** *value*

no ip route-map *route-map-name* [**sequence-number** *number*] **set local-preference** *value*

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>value</i>	Configures the local-preference value for routes being redistributed in to BGP. The value is between 0 and 4294967295.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **set local-preference** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **set** criteria.
- The local preference attribute is used to set preference to an exit point from the local autonomous system (AS).
- If there are multiple exit points from the AS, the local preference attribute is used to select the exit point for a specific route.

Examples

```
-> ip route-map 111 sequence-number 50 set local-preference 4
-> no ip route-map 111 sequence-number 50 set local-preference 4
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[show ip route-map](#)

Displays the configured IP route maps.

MIB Objects

alaRouteMapTable

alaRouteMapIndex

alaRouteMapSequence

alaRouteMapType

alaRouteMapValue

alaRouteMapRowStatus

ip route-map set level

Configures the level of the selected ISIS route.

ip route-map *route-map-name* [**sequence-number** *number*] **set level** {**level1** | **level2** | **level1-2**}

no ip route-map *route-map-name* [**sequence-number** *number*] **set level** {**level1** | **level2** | **level1-2**}

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
level1	Matches IS-IS Level-1 routes only.
level2	Matches IS-IS Level-2 routes only.
level1-2	Matches IS-IS Level1-2 routes.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **set level** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The *route-map-name* and **sequence-number** must exist before you configure this **set** criteria.

Examples

```
-> ip route-map 111 sequence-number 50 set level level1
-> no ip route-map 111 sequence-number 50 set level level1
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[show ip route-map](#)

Displays the configured IP route maps.

MIB Objects

alaRouteMapTable

alaRouteMapIndex

alaRouteMapSequence

alaRouteMapType

alaRouteMapValue

alaRouteMapRowStatus

ip route-map set ip-next-hop

Configures the IP address of the next hop in a route map.

```
ip route-map route-map-name [sequence-number number] set ip-next-hop ip_address
```

```
no ip route-map route-map-name [sequence-number number] set ip-next-hop ip_address
```

Syntax Definitions

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>ip_address</i>	IP address of the next hop.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the **set ip-next-hop** 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-next-hop 128.251.17.224  
-> no ip route-map 222 sequence-number 50 set ip-next-hop 128.251.17.224
```

Release History

Release 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[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

<i>route-map-name</i>	The name of the route map.
<i>number</i>	A number that links together the route maps. The range is 1–100.
<i>ipv6_address</i>	IPv6 address of the next hop.

Defaults

parameter	default
<i>number</i>	50

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced

Related Commands

[ip route-map action](#)

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

[show ip route-map](#)

Displays the configured IP route maps.

MIB Objects

```
alaIPRouteMapTable  
  alaRouteMapIndex  
  alaRouteMapSequence  
  alaRouteMapType  
  alaRouteMapValue  
  alaRouteMapRowStatus
```

vrf

Configures and selects a virtual routing and forwarding (VRF) instance on the switch.

vrf [*name* / **default**]

no vrf *name*

Syntax Definitions

name The alphanumeric name (1–20 characters) assigned to the VRF instance.

default Optional. Selects the default VRF instance.

Defaults

A default VRF instance exists in the switch configuration. All applications that are not VRF aware belong to this instance.

Parameter	Default
<i>name</i> / default	default VRF instance

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a VRF instance. Deleting the default instance is not allowed. In addition, any interfaces configured for a VRF instance are automatically removed when the instance is deleted.
- To return to the default VRF instance from within the context of another instance, enter the **vrf** command with or without the optional **default** parameter (for example, **vrf** or **vrf default**).
- Configuring a VRF instance name is case sensitive. In addition, if the name specified does not exist, a VRF instance is automatically created. As a result, it is possible to create instances or delete a wrong instance accidentally.
- If the name of an existing instance is specified with this command, VRF changes the command prompt to reflect the specified instance name. All CLI commands entered at this point are applied within the context of the active VRF instance.
- It is also possible to configure other instances from within the CLI context of the default VRF instance by entering the **vrf** command followed by the instance name. For example, entering **vrf IpOne ip interface intf100 address 100.1.1.1/24 vlan 100** is applied to the IpOne instance even though IpOne is not the active CLI context.

Examples

```
-> vrf IpOne  
IpOne: ->
```

```
IpOne: -> vrf IpTwo  
IpTwo: ->
```

```
IpTwo: -> vrf  
->
```

```
IpTwo: -> vrf default  
->
```

```
-> vrf IpOne ip interface intf100 address 100.1.1.1/24 vlan 100  
->
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show vrf](#) Displays the VRF instance configuration for the switch.

MIB Objects

```
alaVirtualRouterNameTable  
  alaVirtualRouterName
```

ip export route-map

Configures a route map to export routes from the source VRF to Global Routing Table (GRT). The route-map is used to filter routes. Only those FDB (Forwarding Routing Database) routes that match the conditions of the route map is exported to GRT.

[vrf name] ip export route-map *route-map-name*

[vrf name] no ip export

Syntax Definitions

<i>name</i>	The alphanumeric name (1–20 characters) assigned to the VRF instance. Routes are exported from the specified VRF to GRT.
<i>route-map-name</i>	Name of the configured route map. This route map controls export of routes from the source VRF FDB to GRT.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If VRF is not configured, the routes are exported from the default VRF to GRT.
- Use the **no** form of this command to disable exporting of routes from the VRF to GRT.
- Create a route-map and define protocol preference for the export policy route map by using **ip route-map** command. This route map controls export of routes from the VRF FDB to GRT. Refer to “Configuring IP” chapter in the *OmniSwitch AOS Release 7 Network Configuration Guide* for more information on how to create a route map.
- Route map configured for an export policy can contain any of the following filter and set options:
 - Filter options: ip-address, ip-next-hop, tag, protocol, ipv4-interface, metric, route-type
 - Set option: tag, metric
- Only one route map can be configured as export policy in a VRF.
- You cannot modify a route map that is tagged to an export policy.
- Route leaking between VRFs only supports IPv4 routes.

Examples

```
-> ip export route-map R1
-> vrf vrf2 ip export route-map R1
-> vrf vrf1
```

```
vrfl::-> ip export route-map R1  
-> no ip export R1
```

Release History

Release 7.3.1; command introduced.

Related Commands

vrf	Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match protocol	Matches the protocol specified in the route map with the protocol of the route.
show ip export	Displays the export route configuration details.
show ip global-route-table	Displays the GRT for all the routes that are exported from the VRFs.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIprmConfig  
  alaIprmExportRouteMap
```

ip import vrf

Configures a route map to import routes from GRT to the destination VRF. The route-map is used to filter routes.

```
[vrf name] ip import vrf {name | default} route-map route-map-name
```

```
[vrf name] no ip import vrf {name | default}
```

Syntax Definitions

<i>name</i>	The alphanumeric name (1–20 characters) assigned to the VRF instance.
import vrf <i>name</i>	The export (source) VRF instance name. The routes are imported from the specified VRF.
default	Default VRF. The routes are imported from the default VRF.
<i>route-map-name</i>	Name of the configured route map. This route map controls the import of routes from GRT.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove importing of routes from GRT from the specified export VRF.
- Create a route-map and define protocol preference for the import policy route map by using **ip route-map** command. This route map controls import of routes from GRT. Refer to “Configuring IP” chapter in the *OmniSwitch AOS Release 7 Network Configuration Guide* for more information on how to create a route map.
- Route map configured for the import policy can contain any of the following filter and set options:
 - Filter options: ip-address, ip-next-hop, tag, metric
 - Set option: tag, metric
- Only one route map can be configured for an import policy for each export VRF.
- You cannot modify a route map tagged to an import policy.
- Leaked routes are only for forwarding. If a local route is leaked, that interface is not accessible in the importing VRF. Another switch will not be able to ping the interface in the import VRF.

Examples

```
-> ip import vrf V1 import route-map R2  
-> no ip import VRF V1
```

Release History

Release 7.3.1; command introduced.

Related Commands

vrf	Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match protocol	Matches the protocol specified in the route map with the protocol of the route.
show ip import	Displays the import route configuration details.
show ip global-route-table	Displays the GRT for all the routes that are exported from the VRFs.
show ip route-map	Displays the configured IP route maps.

MIB Objects

```
alaIprmImportVrfTable
  alaIprmImportVrfName
  alaIprmImportVrfRouteMap
  alaIprmImportVrfRowStatus
```

Related Commands

[ip export route-map](#)

Configures a route map to export routes from the source VRF to Global Routing Table (GRT).

[show ip export](#)

Displays the export route configuration details.

MIB Objects

```
alaGrtRouteTable  
  alaGrtGrtVrfName  
  alaGrtRouteDest  
  alaGrtMaskLen  
  alaGrtRouteNextHop  
  alaGrtRouteMetric  
  alaGrtRouteTag
```

arp

Adds a permanent entry to the ARP table. To forward packets, the switch dynamically builds an ARP Table to match the IP address of a device with its physical (MAC) address. These entries age out of the table when the timeout value is exceeded. This command is used to add a permanent entry to the table. Permanent entries do not age out of the table.

```
arp ip_address hardware_address [alias] [arp-name name] [port slot/port] [linkagg agg_num]
```

```
no arp ip_address [alias]
```

Syntax Definitions

<i>ip_address</i>	IP address of the device you are adding to the ARP table.
<i>hardware_address</i>	MAC address of the device in hexadecimal format (for example, 00.00.39.59.f1.0c).
alias	<p>Specifies that the switch will act as an alias (or proxy) for this IP address. When the alias option is used, the switch responds to all ARP requests for the specified IP address with its own MAC address.</p> <p>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.</p>
<i>name</i>	The name to assign to this ARP entry.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a permanent ARP entry.
- Configuring a permanent ARP entry with a multicast address is also supported. This is done by specifying a multicast address for the *ip_address* parameter instead of a unicast address. (OS9000 and OS6850 24-port models only)
- Using the **arp alias** command is not related to proxy ARP as defined in RFC 925. Instead, **arp alias** is similar to the Local Proxy ARP feature, except that it is used to configure the switch as a proxy for only *one* IP address.
- As most hosts support the use of address resolution protocols to determine cache address information (called dynamic address resolution), it is not required 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 7.1.1; command was introduced.

Related Commands

[clear arp-cache](#)

Deletes all dynamic entries from the ARP table.

[ip interface](#)

Enables or disables the Local Proxy ARP feature for an IP interface. When enabled, all traffic within the VLAN is routed. ARP requests return the MAC address of the IP router interface.

[show arp](#)

Displays the ARP table.

MIB Objects

ipNetToMediaTable

- ipNetToMediaIfIndex
- ipNetToMediaNetAddress
- ipNetToMediaPhyAddress
- ipNetToMediaType

alaIpNetToMediaTable

- alaIpNetToMediaPhyAddress
- alaIpNetToMediaProxy

clear arp-cache

Deletes all dynamic entries from the ARP table.

clear arp-cache

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command only clears dynamic entries. If permanent entries have been added to the table, they must be removed using the **no** form of the [ip service](#) command.
- Dynamic entries remain in the ARP table until they time out. The switch uses the MAC Address table timeout value as the ARP timeout value. Use the [mac-learning aging-time](#) command to set the timeout value.

Examples

```
-> clear arp-cache
```

Release History

Release 7.1.1; 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 10K, 6900

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 7.1.1; command introduced

Related Commands

ip service	Adds a permanent entry to the ARP table.
show arp	Displays the ARP table.

MIB Objects

```
alaDoSArpPoisonTable
  alaDoSArpPoisonIpAddr
  alaDosArpPoisonRowStatus
```

arp filter

Configures an ARP filter that determines if ARP Request packets containing a specific IP address are processed by the switch or discarded.

arp filter *ip_address* [**mask** *ip_mask*] [*vlan_id*] [**sender** | **target**] [**allow** | **block**]

no arp filter *ip_address*

Syntax Definitions

<i>ip_address</i>	The IP address to use for filtering ARP packet IP addresses.
<i>ip_mask</i>	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).
<i>vlan_id</i>	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
<i>vlan_id</i>	0 (no VLAN)
<i>ip_mask</i>	255.255.255.255
sender target	target
allow block	block

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

This command 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 7.1.1; 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

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

<i>type</i>	The ICMP packet type. This is conjunction with the ICMP code that determines the type of ICMP message being specified.
<i>code</i>	The ICMP code type. This is conjunction with the ICMP type that determines the type of ICMP message being specified.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
<i>gap</i>	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable disable	disabled
<i>gap</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows the user to enable or disable all types of ICMP messages, and set the minimum packet gap between messages of the specified type.
- 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 pages below. The following ICMP message have specific commands to enable and disable:

ICMP Message	Command
Network unreachable (type 0, code 3)	icmp unreachable
Host unreachable (type 3, code 1)	icmp unreachable
Protocol unreachable (type 3, code 2)	icmp unreachable
Port unreachable (type 3, code 3)	icmp unreachable
Echo reply (type 0, code 0)	icmp echo
Echo request (type 8, code 0)	icmp echo
Timestamp request (type 13, code 0)	icmp timestamp
Timestamp reply (type 14, code 0)	icmp timestamp
Address Mask request (type 17, code 0)	icmp addr-mask
Address Mask reply (type 18, code 0)	icmp addr-mask

- Enabling **Host unreachable** and **Network 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.

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 7.1.1; 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.
<i>gap</i>	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable disable	disabled
<i>gap</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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.
<i>gap</i>	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable disable	enable
<i>gap</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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.
<i>gap</i>	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable disable	enable
<i>gap</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced

Related Commands

show icmp control Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrlTable
  alaIcmpCtrlType
alaIcmpCtrlTable
  alaIcmpCtrlCode
  alaIcmpCtrlStatus
  alaIcmpCtrlPktGap
```

icmp addr-mask

Enables or disables ICMP address mask messages, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

icmp addr-mask [**request** | **reply**] {{**enable** | **disable**} | **min-pkt-gap** *gap*}

Syntax Definitions

request	Specifies request address mask messages.
reply	Specifies reply address mask messages.
enable	Enables the specified ICMP message.
disable	Disables the specified ICMP message.
<i>gap</i>	The number of microseconds required between ICMP messages of this type.

Defaults

parameter	default
enable disable	enable
<i>gap</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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, disable, or set the minimum packet gap for both types.
- The address mask ICMP messages can also be enabled, disabled, and modified using the [icmp type](#) command. See the [icmp type](#) command information on the type and code for the address mask ICMP messages.

Examples

```
-> icmp addr-mask reply enable
-> icmp addr-mask enable
-> icmp addr-mask request enable
-> icmp addr-mask request min-pkt-gap 50
```

Release History

Release 7.1.1; 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

<code>enable</code>	Enables ICMP messages.
<code>disable</code>	Disables ICMP messages.

Defaults

parameter	default
<code>enable disable</code>	<code>enable</code>

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> icmp messages enable
-> icmp messages disable
```

Release History

Release 7.1.1; command introduced

Related Commands

icmp type	Enables or disables a specific type of ICMP message, and sets the minimum packet gap.
show icmp control	Allows the viewing of the ICMP control settings.

MIB Objects

```
alaIcmpCtrl
  alaIcmpAllMsgStatus
```

ip dos scan close-port-penalty

Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP or UDP packet is received on a closed port.

ip dos scan close-port-penalty *penalty_value*

Syntax Definitions

penalty_value A penalty value added to the penalty scan value. This value can be any non-negative integer.

Defaults

parameter	default
<i>penalty_value</i>	10

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>penalty_value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 distinguish between a legal TCP packet and a port scan packet.

Examples

```
-> ip dos scan tcp open-port-penalty 10
```

Release History

Release 7.1.1; 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
<i>penalty_value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 distinguish between a legal UDP packet and a port scan packet.

Examples

```
-> ip dos scan udp open-port-penalty 15
```

Release History

Release 7.1.1; 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
<i>threshold_value</i>	1000

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the total port scan penalty value exceeds this value, a port scan attack is recorded.
- The penalty value is incremented by recording TCP or UDP packets that are bound for open or closed ports. Such packets are given a penalty value, which are added. The commands for setting the packet penalty value are the [ip dos scan close-port-penalty](#), [ip dos scan tcp open-port-penalty](#), and [ip dos scan udp open-port-penalty](#) commands.

Examples

```
-> ip dos scan threshold 1200
```

Release History

Release 7.1.1; command introduced

Related Commands

ip dos scan close-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP or UDP packet is received on a closed port.
ip dos scan tcp open-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP packet is received on an open port.
ip dos scan udp open-port-penalty	Assigns a penalty value to be added to the Denial of Service penalty scan value when a UDP packet is received on an open port.
show ip dos config	Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

alaDoSConfig
 alaDoSPortScanThreshold

ip dos trap

Sets whether the switch generates SNMP DoS traps when an attack is detected.

```
ip dos trap {enable | disable}
```

Syntax Definitions

enable	Enables the generation of DoS traps.
disable	Disables the generation of DoS traps.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>decay_value</i>	2

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

- The statistics show the cumulative totals since the last time the switch was powered on or since the last reset of the switch was executed.
- Packets received on a port that is a member of the UserPorts group are dropped if they contain a source IP network address that does not match the IP subnet for the port. This is done to block spoofed IP traffic. If the UserPorts group function is active and spoofed traffic was detected and blocked, the output display of this command includes statistics regarding the spoofed traffic.
- The presence of spoofing event statistics in the output display of this command indicates that an attack was prevented, not that the switch is currently under attack.
- If statistics for spoofed traffic are not displayed, then a spoofing attempt has not occurred since the last time this command was issued.

Examples

```
-> show ip traffic
```

```
IP statistics
Datagrams received
  Total                = 621883,
  IP header error      = 0,
  Destination IP error = 51752,
  Unknown protocol     = 0,
  Local discards       = 0,
  Delivered to users   = 567330,
  Reassemble needed    = 0,
  Reassembled          = 0,
```



```

Reassemble failed      =          0

Datagrams sent
  Forwarded            =    2801,
  Generated             =   578108,
  Local discards       =          0,
  No route discards    =          9,
  Fragmented           =    2801,
  Fragment failed      =          0,
  Fragments generated  =          0

```

output definitions

Total	Total number of input datagrams received including the datagrams received in the error.
IP header error	Number of IP datagrams discarded due to errors in the IP header (for example, bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discarded in processing IP options).
Destination IP error	Number of IP datagrams discarded because the IP header destination field contained an invalid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E).
Unknown protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Local discards	Number of IP datagrams received that were discarded, even though they had no errors to prevent transmission (for example, lack of buffer space). This does not include any datagrams discarded while awaiting reassembly. This value 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 needed to be reassembled.
Reassembled	Number of IP datagrams received that were successfully reassembled.
Reassemble failed	Number of IP failures detected by the IP reassembly algorithm for all reasons (for example, timed out, error). This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragmented	Number of successfully fragmented IP datagrams.
Fragment failed	Number of packets received and discarded by IP that were not fragmented. This situation can happen if a large packet has the "Don't Fragment" flag set.
Forwarded	Number of IP datagrams forwarded by the switch.
Generated	Total number of IP datagrams that local IP user protocols (including ICMP) generated in response to requests for transmission. This does not include any datagrams counted as "Forwarded."
Local discards	Number of output IP datagrams that were discarded, even though they had no errors to prevent transmission (for example, lack of buffer space). This number includes datagrams counted as "Forwarded" if the packets are discarded for these reasons.

output definitions (continued)

No route discards	Number of IP datagrams received and discarded by IP because no route could be found to transmit them to their destination. This includes any packets counted as “Forwarded” if the packets are discarded for these reasons. It also includes any datagrams that a host cannot route because all of its default routers are down.
Fragments generated	The of IP datagram fragments generated as a result of fragmentation.
Routing entry discards	Number of packets received and discarded by IP even though no problems were encountered to prevent their transmission to their destination (for example, discarded because of lack of buffer space).

Release History

Release 7.1.1; command introduced

Related Commands

[show icmp statistics](#) Displays ICMP statistics and errors.

MIB Objects

N/A

show ip interface

Displays the configuration and status of IP interfaces.

show ip interface [*name* / **emp** | **vlan** *vlan id*]

Syntax Definitions

<i>name</i>	The name associated with the IP interface.
emp	Displays the configuration and status of the Ethernet Management Port interface.
<i>vlan_id</i>	VLAN ID (displays a list of IP interfaces associated with a VLAN).

Defaults

By default, all IP interfaces are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The basic **show ip interface** command displays information about all configured IP interfaces on the switch.
- Use the optional **vlan** parameter to display a list of interfaces configured for the specified VLAN.
- Specify an optional interface *name* to display detailed information about an individual interface.
- Use the optional **emp** parameter to display detailed information about the EMP interface.

Examples

```
-> show ip interface
Total 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
client	60.1.1.1	255.255.255.0	DOWN	NO	vlan 60
gbps	5.5.5.5	255.255.255.0	DOWN	NO	vlan 7
if222	30.1.5.1	255.0.0.0	UP	YES	vlan 222
ldap_client1	173.22.16.115	255.255.255.0	UP	YES	vlan 173
ldap_server1	174.22.16.115	255.255.255.0	UP	YES	vlan 174
radius_client3	110.1.1.101	255.255.255.0	UP	YES	vlan 30
vlan-2	0.0.0.0	0.0.0.0	DOWN	NO	unbound
gre-1	24.24.24.1	255.255.255.0	UP	YES	GRE tunnel
ipip-1	25.25.25.1	255.255.255.0	UP	YES	IPIP tunnel
vlan-23	23.23.23.1	255.255.255.0	UP	YES	vlan 23

output definitions

Name	Interface name. This is the name configured for the interface (for example, Accounting). EMP refers to the Ethernet Management Port. Loopback refers to a loopback interface configured for testing.
IP Address	IP address of the interface. Configured through the ip interface command.
Subnet Mask	IP subnet mask for the interface IP address. Configured through the ip interface command.
Status	Interface status: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • unbound—No device is bound to the interface. • vlan—The VLAN ID that is bound to the interface. • EMP—The Ethernet Management Port is bound to the interface. • Loopback—A loopback interface is configured for testing. • GRE tunnel—GRE tunnel is configured for the interface. • IPIP tunnel—IPIP tunnel is configured for the interface. • vlan<MC>—The multi-chassis virtual IP (VIP) VLAN that is bound to the interface. Configured through the ip interface command. The GRE tunnel and IPIP tunnel devices are supported only on the OmniSwitch 10K switches.

```

-> show ip interface Marketing
Interface Name = Marketing
  SNMP Interface Index      = 13600007,
  IP Address                = 172.16.105.10,
  Subnet Mask               = 255.255.0.0,
  Broadcast Address        = 172.16.255.255,
  Device                    = vlan 200,
  Encapsulation            = eth2,
  Forwarding                = disabled,
  Administrative State     = enabled,
  Operational State        = down,
  Operational State Reason = device-down,
  Router MAC                = 00:d0:95:6a:f4:5c,
  Local Proxy ARP          = disabled,
  Maximum Transfer Unit    = 1500,
  Primary (config/actual)  = no/yes

```

output definitions

SNMP Interface Index	Interface index.
IP Address	IP address associated with the interface. Configured through the ip interface command.
Subnet Mask	IP subnet mask for the interface. Configured through the ip interface command.
Broadcast Address	Broadcast address for the interface.

output definitions (continued)

Device	<p>The type of device bound to the interface:</p> <ul style="list-style-type: none"> • unbound—No device is bound to the interface. • vlan—The VLAN ID that is bound to the interface. • EMP—The Ethernet Management Port is bound to the interface. • Loopback—A loopback interface is configured for testing. • GRE tunnel—GRE tunnel is configured for the interface. • IPIP tunnel—IPIP tunnel is configured for the interface. <p>Configured through the ip interface command.</p> <p>The GRE tunnel and IPIP tunnel devices are supported only on the OmniSwitch 10K switches.</p>
Encapsulation	<p>Displays the IP router encapsulation (eth2 or snap) that the interface uses when routing packets. Configured through the ip interface command.</p>
Forwarding	<p>Indicates whether IP forwarding is active for the interface (enabled or disabled). Configured through the ip interface command.</p>
Administrative State	<p>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.</p>
Operational State	<p>Indicates whether the interface is active (up or down).</p>
Operation State Reason	<p>Indicates why the operational state of the interface is down:</p> <ul style="list-style-type: none"> • 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—The source IP address of the tunnel is invalid. • tunnel-dst-unreachable—The destination IP address of the tunnel is not reachable. <p>The tunnel-src-invalid and tunnel-dst-unreachable Operational State reasons are supported only on the OmniSwitch 10K switches. These two reasons are only applicable for the GRE tunnel and IPIP tunnel device types.</p> <p>Operational State Reason field is only included in the display output when the operational state of the interface is down.</p>
Router MAC	<p>Switch MAC address assigned to the interface. Each interface assigned to the same VLAN shares the same switch MAC address.</p>
Local Proxy ARP	<p>Indicates whether Local Proxy ARP is active for the interface (enabled or disabled). Configured through the ip interface command.</p>
Maximum Transfer Unit	<p>The Maximum Transmission Unit size set for the interface. Configured through the ip interface command.</p>
Primary (config/actual)	<p>Indicates if the interface is the configured and/or actual primary interface for the device (VLAN, EMP, Loopback). If the actual status is set to yes and the config status is set to no, the interface is the default interface for the VLAN. Configured through the ip interface command.</p>

The following are examples of the output display on OmniSwitch 10K switches:

```
-> show ip interface ipip-1
Interface Name = ipip-1
SNMP Interface Index      = 13600001,
IP Address                 = 25.25.25.1,
Subnet Mask                = 255.255.255.0,
Device                    = IPIP Tunnel,
Tunnel Source Address      = 23.23.23.1
Tunnel Destination Address = 23.23.23.2,
Forwarding                 = enabled,
Administrative State       = enabled,
Operational State         = up,
Maximum Transfer Unit      = 1480,
```

```
-> show ip interface gre-1
Interface Name = gre-1
SNMP Interface Index      = 13600002,
IP Address                 = 24.24.24.1,
Subnet Mask                = 255.255.255.0,
Device                    = GRE Tunnel,
Tunnel Source Address      = 23.23.23.1
Tunnel Destination Address = 23.23.23.2,
Forwarding                 = enabled,
Administrative State       = enabled,
Operational State         = down,
Operational State Reason   = unbound,
Maximum Transfer Unit      = 1476,
```

output definitions

SNMP Interface Index	Interface index.
IP Address	IP address associated with the interface. Configured through the ip interface command.
Subnet Mask	IP subnet mask for the interface. Configured through the ip interface command.
Device	The type of device bound to the interface: <ul style="list-style-type: none"> • unbound—No device is bound to the interface. • vlan—The VLAN ID that is bound to the interface. • EMP—The Ethernet Management Port is bound to the interface. • Loopback—A loopback interface is configured for testing. • GRE tunnel—GRE tunnel is configured for the interface. • IPIP tunnel—IPIP tunnel is configured for the interface. Configured through the ip interface command.
Tunnel Source Address	The source IP address for the tunnel.
Tunnel Destination Address	The destination IP address for the tunnel.
Forwarding	Indicates whether 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.

output definitions (continued)

Operational State	Indicates whether the interface is active (up or down).
Operational State Reason	Indicates why the operational state of the interface is down: <ul style="list-style-type: none"> • 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 administrative 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—The source IP address of the tunnel is invalid. • tunnel-dst-unreachable—The destination IP address of the tunnel is not reachable. <p>Operational State Reason field is only included in the display output when the operational state of the interface is down.</p>
Maximum Transfer Unit	The Maximum Transmission Unit size set for the interface. Configured through the ip interface command.

Release History

Release 7.1.1; command introduced

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 tunnel	Configures the end points for the GRE and IPIP tunnels.
show icmp statistics	Displays ICMP statistics and errors.

MIB Objects

```

alaIpInterfaceTable
  alaIpInterfaceName
  alaIpInterfaceAddress
  alaIpInterfaceMask
  alaIpInterfaceAdminState
  alaIpInterfaceDeviceType
  alaIpInterfaceVlanID
  alaIpInterfaceIpForward
  alaIpInterfaceEncap
  alaIpInterfaceLocalProxyArp
  alaIpInterfacePrimCfg
  alaIpInterfaceOperState
  alaIpInterfaceOperReason
  alaIpInterfaceRouterMac
  alaIpInterfaceBcastAddr
  alaIpInterfacePrimAct
  alaIpInterfaceMtu
  alaIpInterfaceTunnelSrc
  alaIpInterfaceTunnelDst

```

show ip routes

Displays the IP Forwarding table.

[vrf name] show ip routes [summary]

Syntax Definitions

name The alphanumeric name (1–20 characters) assigned to the VRF instance.

summary Displays a summary of routing protocols that appear in the IP Forwarding table.

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The IP Forwarding table includes static routes as well as all routes learned through routing protocols (for example, RIP, OSPF).
- Use the optional **summary** keyword to display a list of routing protocols and the number of routes for each protocol that appear in the IP Forwarding table.
- The imported routes are also displayed under the protocol field as **IMPORT** in the show output.

Examples

```
-> show ip routes
```

```
+ = Equal cost multipath routes
Total 4 routes
```

Dest Address	Gateway Addr	Age	Protocol
0.0.0.0/0	10.255.11.254	01:50:33	STATIC
10.255.11.0/24	10.255.11.225	01:50:33	LOCAL
127.0.0.1/32	127.0.0.1	01:51:47	LOCAL
212.109.138.0/24	212.109.138.138	00:33:07	LOCAL
12.0.0.0/8	12.0.0.1	00:20:00	IMPORT

```
-> show ip route summary
```

Protocol	Route Count
Local	3
Static	1
RIP	0
ISIS	0
OSPF	0

BGP	0
Import	1
Other	0
TOTAL =	5

output definitions

Dest Addr	Destination IP address/mask length.
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 <i>hh/mm/ss</i> format. If it is more than a day old, it is displayed in <i>dd/hh</i> 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). 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 7.1.1; command introduced
 Release 7.3.1; **vrf** parameter added.

Related Commands

ping	Used to test whether an IP destination can be reached from the local switch.
traceroute	Used to find the path taken by an IP packet from the local switch to a specified destination.
show ip routes	Displays a list of all routes (static and dynamic) that exist in the IP router database.

MIB Objects

```

ipCidrRouteTable
  ipCidrRouteDest
  ipCidrRouteMask
  ipCidrRouteTos
  ipCidrRouteNextHop
  ipCidrRouteIfIndex
  ipCidrRouteType
  ipCidrRouteProto
  ipCidrRouteAge
  ipCidrRouteInfo
  ipCidrRouteNextHopAS
  ipCidrRouteMetric1
  ipCidrRouteMetric2
  ipCidrRouteMetric3
  ipCidrRouteMetric4
  ipCidrRouteMetric5
  ipCidrRouteStatus
  
```

show ip route-pref

Displays the IPv4 routing preferences of a router.

[vrf name] show ip route-pref

Syntax Definitions

name The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The imported routes are also displayed under the protocol field as IMPORT in the show output.

Examples

```
-> show ip route-pref
  Protocol      Route Preference Value
-----+-----
  Local         1
  Static        2
  OSPF          110
  ISISL1        115
  ISISL2        118
  RIP           120
  EBGp          190
  IBGP          200
  Import        210
```

Release History

Release 7.1.1; command introduced

Release 7.3.1; **vrf** parameter added.

Related Commands

[ip route-pref](#) Configures the route preference of a router.

MIB Objects

```
alaIprmRtPrefTable  
  alaIprmRtPrefEntryType  
  alaIprmRtPrefEntryValue
```

show ip redistrib

Displays the IPv4 route map redistribution configuration.

[vrf name] show ipv4 redistrib [rip | ospf | isis | bgp]

Syntax Definitions

<i>name</i>	The alphanumeric name (1–20 characters) assigned to the VRF instance.
rip	Displays route map redistribution configurations that use RIP as the destination (into) protocol.
ospf	Displays route map redistribution configurations that specify OSPF as the destination (into) protocol.
isis	Displays route map redistribution configurations that specify ISIS as the destination (into) protocol.
bgp	Displays the route map redistribution configurations that specify BGP as the destination (into) protocol at this time.

Defaults

By default, all route map redistribution configurations are shown.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Specify a destination protocol with this command to display only those configurations that redistribute routes into the specified protocol.

Release History

Release 7.1.1; command introduced

Release 7.3.1; **vrf** parameter added.

Examples

```
-> show ip redistrib
```

Source Protocol	Destination Protocol	Status	Route Map
RIP	OSPF	Enabled	ipv4rm
BGP	RIP	Enabled	ipv4rm
IMPORT	RIP	Enabled	ipv4rm

```
-> show ip redist rip
```

Source Protocol	Destination Protocol	Status	Route Map
BGP	RIP	Enabled	ipv4rm
IMPORT	RIP	Enabled	ipv4rm

output definitions

Source Protocol	The protocol from which the routes are learned.
Destination Protocol	The protocol into which the source protocol routes are redistributed.
Status	The administrative status (Enabled or Disabled) of the route map redistribution configuration.
Route Map	The name of the route map that is applied with this redistribution configuration.

Related Commands

ip redist Controls the conditions for redistributing different IPv6 routes between protocols.

MIB Objects

```
alaRouteMapRedistProtoTable
  alaRouteMapRedistSrcProtoId
  alaRouteMapRedistDestProtoId
  alaRouteMapRedistRouteMapIndex
  alaRouteMapRedistStatus
  alaRouteMapRedistAddressType
  alaRouteMapRedistRowStatus
```

show ip access-list

Displays the details of the access list.

show ip access-list [*access-list-name*]

Syntax Definitions

access-list-name Name of the access list.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If the *access-list-name* is not specified in this command, all the access lists are displayed.

Examples

```
-> show ip access-list
```

Name	Address / Prefix Length	Effect	Redistribution 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
```

Name	Address / Prefix Length	Effect	Redistribution 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.
Redistribution Control	Indicates the conditions specified for redistributing the matched routes.

Release History

Release 7.1.1; command was 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 10K, 6900

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 redistrib-control all-subnets permit
  set metric 100 effect replace
```

Release History

Release 7.1.1; command introduced

Related Commands

ip route-map action	Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
ip route-map match ip address	Matches the route with the specified IPv4 address or with addresses contained in an IPv4 access list specified by the access list name.
ip route-map match ipv6 address	Matches the route with the specified IPv6 address or with addresses contained in an IPv6 access list specified by the access list name.
ip route-map match ip-nexthop	Matches the routes that have a next-hop router address permitted by the specified access list.
ip route-map match ipv6-nexthop	Matches the routes that have an IPv6 next-hop router address permitted by the specified access list.
ip route-map match tag	Permits or denies a route based on the specified next-hop IP address.
ip route-map match tag	Matches the tag value specified in the route map with the one that the routing protocol learned the route on.
ip route-map match metric	Matches the metric value specified in the route map with the one that the routing protocol learned the route on.
ip route-map match route-type	Matches the specified route type with the one that the routing protocol learned the route on.

MIB Objects

```
alaRouteMapRedistProtoTable
  alaRouteMapRedistRouteMapIndex
alaRouteMapTable
  alaRouteMapIndex
  alaRouteMapSequence
  alaRouteMapType
  alaRouteMapValue
  alaRouteMapRowStatus
```

show ip router database

Displays a list of all routes (static and dynamic) that exist in the IP router database. This database serves as a central repository where routes are first processed and where duplicate routes are compared to determine the best route for the Forwarding Routing Database. If a route does not appear in the IP router database list, then the switch does not know about it. In the case of dynamically learned routes, this could indicate that the route was never received by the switch.

```
[vrf name] show ip router database [protocol type / gateway ip_address / dest {ip_address/prefixLen / ip_address}]
```

Syntax Definitions

<i>name</i>	The alphanumeric name (1–20 characters) assigned to the VRF instance.
<i>type</i>	Routing protocol type (local, static, OSPF, RIP, or BGP).
<i>ip_address</i>	Destination IP address.
<i>ip_address/prefixLen</i>	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 10K, 6900

Usage Guidelines

- Command options are not mutually exclusive. You can use them on the same command line to narrow and/or customize the output display of this command. For example, use the **protocol** and **dest** options to display only those routes that are of a specific protocol type and have the specified destination network.
- The IP forwarding table is derived from IP router database processing performed by the switch and contains only unique routes that the switch currently uses. Use the **show ip route** command to view the forwarding table.
- If an expected route does not appear in the IP forwarding table, use the **show ip router database** command to see if the switch knows about the route and/or if a duplicate route with a higher precedence was selected instead.
- The switch compares the protocol of duplicate routes to determine which one to use. Regardless of whether a route has a higher priority metric value, protocol determines precedence. Local routes are given the highest level of precedence followed by static, OSFP, RIP, then BGP routes. As a result, a route that is known to the switch does 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.
- The imported routes are also displayed under the protocol field as IMPORT in the show output.

Examples

-> show ip router database

Destination	Gateway	Interface	Protocol	Metric	Tag	Misc-Info
10.212.31.0/24	10.212.60.27	I1	OSPF	2	0	
10.212.31.0/24	10.212.61.27	I2	OSPF	2	0	
10.212.59.0/24	10.212.59.17	I3	LOCAL	1	0	
10.212.60.0/24	10.212.60.17	I1	LOCAL	1	0	
10.212.61.0/24	10.212.61.17	I2	LOCAL	1	0	
10.212.62.0/24	10.212.60.27	I1	OSPF	2	0	
10.212.62.0/24	10.212.61.27	I2	OSPF	2	0	
10.212.63.0/24	10.212.60.27	I1	OSPF	2	0	
10.212.63.0/24	10.212.61.27	I2	OSPF	2	0	
10.212.66.0/24	10.212.66.17	I4	LOCAL	1	0	
143.209.92.0/24	172.28.6.254	I5	STATIC	1	0	
172.28.6.0/24	172.28.6.2	I5	LOCAL	1	0	
192.168.6.0/24	11.0.0.2	V1	IMPORT	1	0	
192.168.6.0/24	11.0.0.2	v1	IMPORT	1	0	
192.168.6.0/24	11.0.0.3	v1	IMPORT	1	0	

Inactive Static Routes

Destination	Gateway	Metric	Tag	Misc-Info
1.0.0.0/8	8.4.5.3	1	0	

-> show ip router database dest 10.212.62.0/24 protocol ospf

Destination	Gateway	Interface	Protocol	Metric	Tag	Misc-Info
10.212.62.0/24	10.212.60.27	I1	OSPF	2	0	
10.212.62.0/24	10.212.61.27	I2	OSPF	2	0	

Inactive Static Routes

Destination	Gateway	Metric	Tag	Misc-Info
1.0.0.0/8	8.4.5.3	1	0	

Destination Gateway Metric

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.
Interface	The interface associated with the gateway.
Protocol	Protocol by which this IP address was learned: LOCAL, STATIC, OSPF, RIP, BGP).
Metric	RIP metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.
Tag	The tag associated with the route.
Misc-Info	Any additional information about the route.

Release History

Release 7.1.1; command introduced
Release 7.3.1; **vrf** parameter added.

Related Commands

[show ip routes](#) Displays the IP Forwarding table.

MIB Objects

```
alaIprmRouteTable
  alaIprmRouteDest
  alaIprmRouteMask
  alaIprmRouteTos
  alaIprmRouteNextHop
  alaIprmRouteProto
  alaIprmRouteMetric
  alaIprmRoutePriority
```

show ip emp-routes

Displays the IP routes associated with the Ethernet Management Port (EMP).

show ip emp-routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command displays the routes that are connected to the Ethernet Management Port (EMP).
- The EMP cannot handle routing protocols such as RIP or OSPF.
- The default route for the switch cannot be set up on the EMP.

Examples

```
-> show ip emp-routes
```

Dest Address	Subnet Mask	Gateway Addr	Age	Protocol
127.0.0.1	255.255.255.255	127.0.0.1	2d 4h	LOCAL
172.17.1.10	255.255.255.255	10.255.11.225	1d 5h	LOCAL

output definitions

Dest Addr	Destination IP address.
Subnet Mask	Destination IP address IP subnet mask.
Gateway Addr	IP address of the gateway from which this address was learned.
Age	Age of the entry. If the entry is less than a day old, it is displayed in <i>hh/mm/ss</i> format. If it is more than a day old, it is displayed in <i>dd/hh</i> format (for example, a route that is 2 days and 12 hours old is displayed as 2d12h).
Protocol	Protocol by which this IP address was learned (for example, RIP). NETMGT indicates a static route. LOCAL indicates a local interface.

Release History

Release 7.1.1; command introduced

Related Commands**ping**

Tests whether an IP destination can be reached from the local switch.

traceroute

Finds the path taken by an IP packet from the local switch to a specified destination.

show ip config

Displays IP configuration parameters.

show ip config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip config
IP directed-broadcast = OFF,
IP default TTL       = 64
```

output definitions

IP directed-broadcast	Indicates whether the IP directed-broadcast feature is on or off.
IP default TTL	IP default TTL interval.

Release History

Release 7.1.1; command introduced

Related Commands

- [ip directed-broadcast](#) Enables or disables IP directed broadcasts routed through the switch.
- [ip default-ttl](#) Sets TTL value for IP packets.
-

show ip protocols

Displays switch routing protocol information and status.

show ip protocols

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip protocols
```

```
IP Protocols
```

```
RIP status                = Not Loaded,
OSPF status                = Loaded,
ISIS status                = Not Loaded,
BGP status                 = Loaded,
PIM status                 = Loaded,
DVMRP status               = Not Loaded,
RIPng status               = Not Loaded,
OSPF3 status               = Loaded,
```

output definitions

RIP status	Whether RIP is loaded or not.
OSPF status	Whether OSPF is loaded or not.
BGP status	Whether BGP is loaded or not.
DVMRP status	Whether DVMRP is loaded or not.
PIMSM status	Whether PIMSM is loaded or not.
RIPng status	Whether RIP is loaded or not.
OSPF3 status	Whether OSPFv3 is loaded or not.

Release History

Release 7.1.1; 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 router-id

Displays the primary IP address and router ID of the switch, if configured.

show ip router-id

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip router-id
Router ID    = 1.1.1.1,
Primary addr = 31.0.0.1
```

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.

Release History

Release 7.1.1; 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 status of TCP/UDP service ports.

show ip service

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The display output from this command also includes the service port number.

Examples

```
-> show ip service
```

Name	Port	Status
ftp	21	enabled
ssh	22	disabled
telnet	23	disabled
udp-relay	67	disabled
http	80	disabled
network-time	123	disabled
snmp	161	disabled
avlan-telnet	259	disabled
avlan-http	260	disabled
avlan-secure-http	261	disabled
secure_http	443	enabled
proprietary	1024	disabled
proprietary	1025	disabled

output definitions

Name	Name of the TCP/UDP service.
Port	The TCP/UDP well-known port number associated with the service.
Status	The status of the well-known service port: enabled (port is closed) or disabled (port is open).

Release History

Release 7.1.1; command introduced

Related Commands

[ip service](#)

Enables (opens) or disables (closes) well-known TCP/UDP service ports.

MIB Objects

```
alaIpServiceTable
  alaIpServiceType
  alaIpServicePort
  alaIpServiceStatus
alaIpPortServiceTable
  alaIpPortServicePort
  alaIpPortServiceStatus
```

show ip 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 10K, 6900

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 7.1.1; command introduced

Related Commands

ip dos arp-poison restricted-address Adds or deletes an ARP Poison restricted address.

MIB Objects

```
alaDoSArpPoisonTable
  alaDoSArpPoisonIpAddr
  alaDoSArpPoisonDetected
```

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 10K, 6900

Usage Guidelines

Use the basic command (**show arp**) to view all of the entries in the table. Enter a specific IP address or MAC address to view a specific entry.

Examples

```
-> show arp
Total 8 arp entries
Flags (P=Proxy, A=Authentication, V=VRRP)
```

IP Addr	Hardware Addr	Type	Flags	Port	Interface
10.255.11.59	00:50:04:b2:c9:ee	DYNAMIC		3/20	vlan 1
10.255.11.48	00:50:04:b2:ca:11	DYNAMIC		3/20	vlan 1
10.255.11.201	00:10:83:03:e7:e4	DYNAMIC		3/20	vlan 1
10.255.11.14	00:10:5a:04:19:a7	DYNAMIC		3/20	vlan 1
10.255.11.64	00:b0:d0:62:fa:f1	DYNAMIC		3/20	vlan 1
10.255.11.25	00:b0:d0:42:80:24	DYNAMIC		3/20	vlan 1
10.255.11.26	00:b0:d0:42:82:59	DYNAMIC		3/20	vlan 1
10.255.11.254	00:20:da:db:00:47	DYNAMIC		3/20	vlan 1

output definitions

IP Address	Device IP address.
Hardware Addr	MAC address of the device that corresponds to the IP address.
Type	Indicates whether the ARP cache entries are dynamic or static.
Flags	Indicates the type of entry: <ul style="list-style-type: none"> • P = Proxy • A = Authentication (AVLAN) • V = VRRP

output definitions (continued)

Port	The port on the switch attached to the device identified by the IP address.
Interface	The interface to which the entry belongs (for example, VLAN, EMP).

Release History

Release 7.1.1; command introduced

Related Commands

ip service	Adds a permanent entry to the ARP table.
clear arp-cache	Deletes all dynamic entries from the ARP table.

MIB Objects

```
ipNetToMediaTable
  ipNetToMediaIfIndex
  ipNetToMediaNetAddress
  ipNetToMediaPhyAddress
  ipNetToMediaType
ipNetToMediaAugTable
  ipNetToMediaSlot
  ipNetToMediaPort
alaIpNetToMediaTable
  alaIpNetToMediaPhyAddress
  alaIpNetToMediaProxy
  alaIpNetToMediaVRRP
  alaIpNetToMediaAuth
```

show arp 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 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

Use this command to view the status of the various ICMP messages. It is also useful to determine the type and code of the less common ICMP messages.

Examples

```
-> show icmp control
```

Name	Type	Code	Status	min-pkt-gap(us)
echo reply	0	0	enabled	0
network unreachable	3	0	enabled	0
host unreachable	3	1	enabled	0
protocal unreachable	3	2	enabled	0
port unreachable	3	3	enabled	0
frag needed but DF bit set	3	4	enabled	0
source route failed	3	5	enabled	0
destination network unknown	3	6	enabled	0
destination host unknown	3	7	enabled	0
source host isolated	3	8	enabled	0
dest network admin prohibited	3	9	enabled	0
host admin prohibited by filter	3	10	enabled	0
network unreachable for TOS	3	11	enabled	0
host unreachable for TOS	3	12	enabled	0
source quench	4	0	enabled	0
redirect for network	5	0	enabled	0
redirect for host	5	1	enabled	0
redirect for TOS and network	5	2	enabled	0
redirect for TOS and host	5	3	enabled	0
echo request	8	0	enabled	0
router advertisement	9	0	enabled	0
router solicitation	10	0	enabled	0
time exceeded during transmit	11	0	enabled	0
time exceeded during reassembly	11	1	enabled	0
ip header bad	12	0	enabled	0
required option missing	12	1	enabled	0
timestamp request	13	0	enabled	0

timestamp reply	14	0	enabled	0
information request(obsolete)	15	0	enabled	0
information reply(obsolete)	16	0	enabled	0
address mask request	17	0	enabled	0
address mask reply	18	0	enabled	0

output definitions

Name	The name of the ICMP message.
Type	The ICMP message type. This along with the ICMP code specifies the ICMP message.
Code	The ICMP message code. This along with the ICMP type specifies the 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 7.1.1; command introduced

Related Commands

icmp type	Enables or disables a specific type of ICMP message, and sets the minimum packet gap.
icmp unreachable	Enables or disables ICMP messages pertaining to unreachable destinations, and sets the minimum packet gap.
icmp echo	Enables or disables ICMP echo messages, and sets the minimum packet gap.
icmp timestamp	Enables or disables ICMP timestamp messages, and sets the minimum packet gap.
icmp addr-mask	Enables or disables ICMP address mask messages, and sets the minimum packet gap.
icmp messages	Enables or disables all ICMP messages.

show icmp statistics

Displays Internet Control Message Protocol (ICMP) statistics and errors. ICMP is a network layer protocol within the IP protocol suite that provides message packets to report errors and other IP packet processing information back to the source. ICMP generates several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages.

show icmp [statistics]

Syntax Definitions

statistics Optional syntax.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the ICMP Table to monitor and troubleshoot the switch.

Examples

```
-> show icmp
Messages                Received      Sent
-----+-----+-----
Total                   2105         2105
Error                   0            0
Destination unreachable 0            0
Time exceeded          0            0
Parameter problem      0            0
Source quench          0            0
Redirect               0            0
Echo request           2105         0
Echo reply             0           2105
Time stamp request     0            0
Time stamp reply       0            0
Address mask request   0            0
Address mask reply     0            0
```

output definitions

Total	Total number of ICMP messages the switch received or attempted to send. This counter also includes all the messages that were counted as errors.
Error	Number of ICMP messages the switch sent/received but was unable to process because of ICMP-specific errors (for example, bad ICMP checksums, bad length).

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 occur when a packet is dropped because the TTL counter reaches zero. When a large number of these messages occur, it is a symptom that packets are looping, that congestion is severe, or that the TTL counter value is set too low. These messages also occur when all the fragments trying to be reassembled do not arrive before the reassembly timer expires.
Parameter problem	Number of messages sent/received which indicate that an illegal value has been detected in a header field. These messages can indicate a problem in the sending IP software of the host or gateway.
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 7.1.1; command introduced

Related Commands

[show udp statistics](#) Displays UDP errors and statistics.

show tcp statistics

Displays TCP statistics.

show tcp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 the error. This count includes segments received on currently established connections.
Error segments received	Total number of segments received in error (for example, bad TCP checksums).
Total segments sent	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Segments retransmitted	Number of TCP segments transmitted containing one or more previously transmitted octets.
Reset segments sent	Number of TCP segments containing the reset flag.
Connections initiated	Number of connections attempted.
Connections accepted	Number of connections allowed.
Connections established	Number of successful connections.

output definitions (continued)

Attempt fails	Number of times attempted TCP connections have failed.
Established resets	Number of times TCP connections have been reset from the "Established" or "Close Wait" state to the "Closed" state.

Release History

Release 7.1.1; command introduced

Related Commands

show icmp statistics	Displays ICMP statistics and errors.
show tcp ports	Displays the TCP connection table.

show tcp ports

Displays the TCP connection table.

show tcp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 it accepts connections for any IP interface associated with the node. The 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 7.1.1; command introduced

Related Commands

[show ip interface](#)

Displays the status and configuration of IP interfaces.

[show tcp statistics](#)

Displays TCP statistics.

show udp statistics

Displays UDP errors and statistics.

show udp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced

Related Commands

[show udp ports](#) Displays the UDP Listener table.

show udp ports

Displays the UDP Listener table. The table shows the local IP addresses and the local port number for each UDP listener.

show udp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced

Related Commands

[show udp statistics](#) Displays UDP errors and statistics.

show ip dos config

Displays the configuration parameters of the DoS scan for the switch.

show ip dos config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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
DoS trap generation	= ENABLED,
DoS port scan threshold	= 1000,
DoS port scan decay	= 2,
DoS port scan close port penalty	= 10,
DoS port scan TCP open port penalty	= 0,
DoS port scan UDP open port penalty	= 0,
Dos MAXimum Ping Rate	= 100
Dos Maximum ARP Request Rate	= 500

output definitions

DoS trap generation	Displays the status of DoS trap generation. It is either ENABLED or DISABLED . This is set using the ip dos trap command.
DoS port scan threshold	The penalty threshold setting. When enough packets have increased the penalty number to this setting, a trap is generated to warn the administrator that a DoS attack is in progress. This is set using the ip dos scan threshold command.
DoS port scan decay	The decay value for the switch. The penalty value of the switch is decreased by this number every minute. This is set using the ip dos scan decay command.
DoS port scan close port penalty	The penalty value for packets received on closed UDP and TCP ports. The penalty number for the switch is increased by this amount every time a packet is received on a closed UDP or TCP port. This is set using the ip dos scan close-port-penalty command.
DoS port scan TCP open port penalty	The penalty value for packets received on open TCP ports. The penalty number for the switch is increased by this amount every time a packet is received on an open TCP port. This is set using the ip dos scan tcp open-port-penalty command.
DoS port scan UDP open port penalty	The penalty value for packets received on open UDP ports. The penalty number for the switch is increased by this amount every time a packet is received on an open UDP port. This is set using the ip dos scan udp open-port-penalty command.

Release History

Release 7.1.1; 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 10K, 6900

Usage Guidelines

- This command displays the number of attacks the switch has detected for several types of DoS attacks.
- If an attack is detected and reported, it does not necessarily mean that an attack occurred. The switch assumes a DoS attack is underway anytime the penalty threshold is exceeded. It is possible for this threshold to be exceeded when no attack is in progress.

Examples

```
-> show ip dos statistics
DoS type           Attacks detected
-----+-----
port scan          0
tcp sync flood     0
ping of death      0
smurf              0
pepsi              0
land               0
teardrop/bonk/boink 0
loopback-src       0
invalid-ip         0
invalid-multicast  0
unicast dest-ip/multicast-mac 0
ping overload      0
arp flood          0
```

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 7.1.1; command introduced

Related Commands**show ip dos config**

Displays the configuration parameters of the DoS scan for the switch.

MIB Objects

alaDoSTable

alaDoSType

show vrf

Displays the Multiple VRF instance configuration for the switch.

show vrf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Information is displayed for all VRF instances configured on the switch.

Examples

```
-> show vrf
Virtual Routers   Protocols
-----
      default
      IpOne     RIP
      IpTwo     BGP
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrf Configures a Multiple VRF instance for the switch.

MIB Objects

```
alaVirtualRouterNameTable
  alaVirtualRouterNameIndex
  alaVirtualRouterName
```

14 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

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	<ul style="list-style-type: none"> ipv6 interface ipv6 address ipv6 address global-id ipv6 address local-unicast ipv6 dad-check ipv6 hop-limit ipv6 pmtu-lifetime ipv6 neighbor stale-lifetime ipv6 neighbor ipv6 prefix ipv6 static-route ipv6 static-route ipv6 route-pref ipv6 virtual-source-mac ipv6 virtual-source-mac tracertoe6 show ipv6 icmp statistics show ipv6 interface show 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 listeners show ipv6 tcp connections show ipv6 tunnel configured show ipv6 tunnel 6to4 show ipv6 information
IPv6 Route Map Redistribution	<ul style="list-style-type: none"> ipv6 redistrib ipv6 access-list ipv6 access-list address show ipv6 redistrib show ipv6 access-list
IPv6 RIP	<ul style="list-style-type: none"> ipv6 load rip ipv6 rip admin-state ipv6 rip invalid-timer ipv6 rip garbage-timer ipv6 rip holddown-timer ipv6 rip jitter ipv6 rip route-tag ipv6 rip update-interval ipv6 rip triggered-sends ipv6 rip interface ipv6 rip interface metric ipv6 rip interface recv-status ipv6 rip interface send-status ipv6 rip interface horizon show ipv6 rip show ipv6 rip interface show ipv6 rip peer show ipv6 rip routes

ipv6 interface

Configures an IPv6 interface on a VLAN or IPv6 tunnel.

```

ipv6 interface if_name [vlan vid | tunnel {tid | 6to4}] admin-state [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-min-interval interval | no ra-min-interval]
[ra-clock-skew time]
[ra-send-mtu] {yes | no}
[mtu size]
[retrans-timer time]
[dad-transmits count]
[ra-hop-limit count]

no ipv6 interface if_name

```

Syntax Definitions

<i>if_name</i>	IPv6 interface name.
vlan	Identifies a VLAN interface.
<i>vid</i>	VLAN ID number.
tunnel	Identifies a configured tunnel interface.
<i>tid</i>	Tunnel ID number.
6to4	Identifies the 6to4 tunnel interface.
base-reachable-time <i>time</i>	Base value used to compute the reachable time for neighbors reached through this interface.
ra-send	Specifies whether the router advertisements are sent on this interface.
ra-max-interval <i>interval</i>	Maximum time, in seconds, allowed between the transmission of unsolicited multicast router advertisements in this interface. The range is 4 - 1,800.
ra-managed-config-flag	Value to be placed in the managed address configuration flag field in router advertisements sent on this interface.
ra-other-config-flag	Value to be placed in the other stateful configuration flag in router advertisements sent on this interface.
ra-reachable-time <i>time</i>	Value, in milliseconds, to be placed in the reachable time field in router advertisements sent on this interface. The range is 0 - 3,600,000. The special value of zero indicates that this time is unspecified by the router.

ra-retrans-timer <i>time</i>	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.
mtu <i>size</i>	The maximum transmission unit for a tunnel interface. Use the vlan command's mtu-ip to set for a VLAN.
retrans-timer <i>time</i>	The amount of time, in milliseconds, between retransmission of a neighbor solicitation during neighbor discovery.
dad-transmits <i>count</i>	The number of neighbor solocitations to send during Duplicate Address Detection.
ra-hop-limit <i>count</i>	The value placed in the current hop limit field of router advertisements sent on this interface.
ra-default-lifetime <i>time</i>	Value, in seconds, to be placed in the router lifetime field in router advertisements sent on this interface. The time must be zero or between the value of "ra-max-interval" and 9,000 seconds. A value of zero indicates that the router is not to be used as a default router. The "no ra-default-lifetime" option will calculate the value using the formula (3 * ra-max-interval).
ra-min-interval <i>interval</i>	Value, in seconds, allowed between the transmission of unsolicited multicast router advertisements on this interface. The interval must be a minimum of 3 and not more than .75 times the value of ra-max-interval. The "no ra-min-interval" option will calculate the value using the formula (.33 * ra-max-interval).
ra-clock-skew <i>time</i>	Value, in seconds. The router advertisement clock skew allows the link propagation delays and poorly synchronized clocks on routers participating in router discover over this interface. The timer differences that fall within the clock skew value are treated as valid times.
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	calculated
ra-min-interval	calculated
ra-send-mtu	no
ra-clock-skew	600
base-reachable-time	360
retrans-timer	1000
dad-transmits	1
ra-other-config-flag	false
ra-hop-limit	64

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete an interface.
- When you create an IPv6 interface, it is enabled by default.
- All IPv6 VLAN and tunnel interfaces must have a name.
- When creating an IPv6 interface you must specify a VLAN ID or Tunnel 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.
- A default **6to4** tunnel named “tunnel_6to4” is automatically created. It can only be enabled/disabled or its configuration modified, it cannot be deleted.
- A 6to4 interface cannot send advertisements (**ra-send**).
- To enable IPv6 routing you must first create a VLAN, then create an IPv6 interface on the VLAN. See [Chapter 4, “VLAN Management Commands,”](#) for information on creating VLANs.
- To route IPv6 traffic over an IPv4 network, you must create an IPv6 tunnel using the [ipv6 interface](#) command.

Examples

```
-> ipv6 interface Test vlan 1
-> ipv6 interface Test_Tunnel tunnel 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 interface	Displays IPv6 Interface Table.
show ipv6 tunnel configured	Displays IPv6 Configured Tunnel.
show ipv6 tunnel 6to4	Displays IPv6 6to4 tunnel information.

MIB Objects

IPv6Ifindex

```
alaIPv6InterfaceTable
  alaIPv6InterfaceName
  alaIPv6InterfaceMtu
  alaIPv6InterfaceSendRouterAdvertisements
  alaIPv6InterfaceMaxRtrAdvInterval
  alaIPv6InterfaceAdvManagedFlag
  alaIPv6InterfaceAdvOtherConfigFlag
  alaIPv6InterfaceAdvRetransTimer
  alaIPv6InterfaceAdvDefaultLifetime
  alaIPv6InterfaceAdminStatus
  alaIPv6InterfaceAdvReachableTime
  alaIPv6InterfaceBaseReachableTime
  alaIPv6InterfaceAdvSendMtu
  alaIPv6InterfaceRowStatus
```

ipv6 interface tunnel source destination

Configures the source and destination IPv4 addresses for a configured tunnel.

```
ipv6 interface if_name tunnel {[source ipv4_source] [destination ipv4_destination]}
```

Syntax Definitions

<i>if_name</i>	Name assigned to the tunnel interface.
<i>ipv4_source</i>	Source IPv4 address for the configured tunnel.
<i>ipv4_destination</i>	Destination IPv4 address for the configured tunnel.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **ipv6 interface** command to create an IPv6 tunnel interface.
- A configured tunnel interface cannot be enabled until both its v4 source and destination addresses have been specified.

Examples

```
-> ipv6 interface Test tunnel 2 source 192.0.2.1 destination 198.51.100.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 interface	Creates an IPv6 tunnel interface.
show ipv6 tunnel configured	Displays IPv6 tunnel information.

MIB Objects

```
IPv6IfIndex  
  alaIPv6ConfigTunnelv4Source  
  alaIPv6ConfigTunnelv4Dest  
  alaIPv6ConfigTunnelRowStatus
```

ipv6 address

Configures an IPv6 address for an IPv6 interface on a VLAN, configured tunnel, or a 6to4 tunnel. There are different formats for this command depending on the address type.

```
ipv6 address ipv6_address /prefix_length [anycast] {if_name | loopback}
```

```
no ipv6 address ipv6_address [anycast] {if_name | loopback}
```

```
ipv6 address ipv6_prefix eui-64 {if_name | loopback}
```

```
no ipv6 address ipv6_prefix eui-64 {if_name | loopback}
```

Syntax Definitions

<i>ipv6_address</i>	IPv6 address.
<i>/prefix_length</i>	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.
<i>if_name</i>	Name assigned to the interface.
loopback	Configures the loopback interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete an address.
- You can assign multiple IPv6 addresses to an IPv6 interface.
- No default value for prefix length.
- The “eui” form of the command is used to add or remove an IPv6 address for a VLAN or configured tunnel using an EUI-64 interface ID in the low order 64 bits of the address.

Examples

```
-> ipv6 address 2001:DB8:4132:86::19A/64 Test_Lab  
-> ipv6 address 2002:C633:6489::35/64 Test_6to4
```

Release History

Release 7.1.1; 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 address global-id

Automatically generates or allows a new global ID to be entered.

```
ipv6 address global-id {generate | globalID}
```

Syntax Definitions

generate	Automatically generates the global ID.
<i>globalID</i>	A 5-byte global ID value specified in the form hh:hhh:hhh

Defaults

By default, the IPv6 global ID is set to all zeros.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Global ID needs to be automatically generated or configured explicitly.
- A 40-bit global identifier is used to make the local IPv6 address prefixes globally unique.
- The global ID will be generated the first time a local unicast address is added through the [ipv6 address local-unicast](#) command or when the [ipv6 address global-id](#) command is executed.

Examples

```
-> ipv6 address global-id generate
-> ipv6 address global-id 32:57a3:8fed
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 address local-unicast	Creates a IPv6 local unicast address using the configured global ID.
ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

alaIPv6GlobalID

ipv6 address local-unicast

Creates a IPv6 local unicast address using the configured global ID.

ipv6 address local-unicast [**global-id** *globalID*] [**subnet-id** *subnetID*] [**interface-id** *interfaceID* | **eui-64**] [**prefix-length** *prefixLength*] [*if-name* | **loopback**]

[no] ipv6 address local-unicast [**global-id** *globalID*] [**subnet-id** *subnetID*] [**interface-id** *interfaceID* | **eui-64**] [**prefix-length** *prefixLength*] [*if-name* | **loopback**]

Syntax Definitions

<i>globalID</i>	A 5-byte global ID value specified in the form hh:hhh:hhh.
<i>subnetID</i>	A 2-byte Subnet ID specified in the form 0xhhhh. The valid range is 0x0000-0xffff or 0-65535.
<i>interfaceID</i>	An interface identifier specified in the form hhhh:hhh:hhh:hhh.
eui-64	Automatically-generated EUI-64 value to be used for interface identifier.
<i>prefixLength</i>	The number of bits that are significant in the IPv6 address (mask). The valid range is 0-128; however, the default value should rarely be overridden.
<i>if-name</i>	The name assigned to the interface.
loopback	The loopback for the loopback interface.

Defaults

parameter	default
<i>prefixLength</i>	64

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the local unicast address. However, addresses are normally deleted using the **ipv6 address** command.
- If the global ID value is not explicitly specified, the default global ID set by the **ipv6 address global-id** command is used.
- If the global ID value is explicitly configured using the **ipv6 address local-unicast** command, the address' global ID will not be changed if the **ipv6 address global-id** command is executed.
- The use of a double-colon abbreviation for the interface identifier similar to that used for full IPv6 addresses is allowed.

Examples

```
-> ipv6 address local-unicast global-id 0073:110:255 subnet-id 23 interface-id  
215:60ff:fe7a:adc0 prefix-length 64 loopback
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 address global-id Automatically generates or allows a new global ID to be entered.

.

show ipv6 information Displays IPv6 information.

MIB Objects

```
alaIPv6LocalUnicastGlobalID  
alaIPv6LocalUnicastSubnetID  
alaIPv6LocalUnicastInterfaceID  
alaIPv6LocalUnicastEUI64  
alaIPv6LocalUnicastPrefixLength
```

ipv6 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

<i>ipv6_address</i>	IPv6 address.
<i>ip_name</i>	Name assigned to the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The switch performs DAD check when an interface is attached 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 2001:db8::1/32 Test_Lab
```

Release History

Release 7.1.1; 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
<i>value</i>	64

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>time</i>	10

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ipv6 pmtu-lifetime 30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 pmtu table](#) Displays the IPv6 path MTU Table.
[show ipv6 information](#) Displays IPv6 information.

MIB Objects

alaIPv6ConfigTable
alaIPv6PMTUMinLifetime

ipv6 neighbor stale-lifetime

Configures the minimum lifetime for neighbors in the unconfirmed state.

ipv6 neighbor stale-lifetime *stale-lifetime*

Syntax Definitions

stale-lifetime Minimum lifetime for neighbor entries in the stale state (5–2800).

Defaults

parameter	default
<i>stale-lifetime</i>	10

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ipv6 neighbor stale-lifetime 1400
```

Release History

Release 7.1.1; 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} {port slot/port/linkagg num}*

no ipv6 neighbor *ipv6_address {if_name}*

Syntax Definitions

<i>ipv6_address</i>	IPv6 address that corresponds to the hardware address.
<i>hardware_address</i>	MAC address in hex format (e.g., 00:00:39:59:F1:0C).
<i>if_name</i>	Name assigned to the interface on which the neighbor resides.
<i>slot/port</i>	Slot/port used to reach the neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 port 1/1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 neighbors](#) Displays IPv6 Neighbor Table.

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

<i>ipv6_address</i>	IPv6 address of the interface.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask). (1...127).
valid-lifetime <i>time</i>	Length of time, in seconds, that this prefix will remain valid, i.e. time until deprecation. A value of 4,294,967,295 represents infinity.
preferred-lifetime <i>time</i>	Length of time, in seconds, that this prefix will remain preferred, i.e. time until deprecation. A value of 4,294,967,295 represents infinity.
on-link-flag	On-link configuration flag. When “true” this prefix can be used for on-link determination.
autonomous-flag	Autonomous address configuration flag. When “true”, indicates that this prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
<i>if_name</i>	Name assigned to the interface.

Defaults

parameter	default
valid-lifetime <i>time</i>	2,592,000
preferred-lifetime <i>time</i>	604,800
on-link-flag	true
autonomous-flag	true

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to delete a prefix.

Examples

```
-> ipv6 prefix 4132:86::/64 Test
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 prefixes Displays IPv6 prefixes used in router advertisements.

MIB Objects

```
IPv6IfIndex  
alaIPv6InterfacePrefixTable  
  alaIPv6InterfacePrefix  
  alaIPv6InterfacePrefixLength  
  alaIPv6InterfacePrefixValidLifetime  
  alaIPv6InterfacePrefixPreferredLifetime  
  alaIPv6InterfacePrefixonLinkFlag  
  alaIPv6InterfacePrefixAutonomousFlag  
  alaIPv6InterfacePrefixRowStatus
```

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

<i>ipv6_prefix</i>	IPv6 network that is the destination of this static route.
<i>/prefix_length</i>	The number of bits (0...128) that are significant in the IPv6 address (mask).
gateway <i>ipv6_address</i>	IPv6 address of the next hop used to reach the destination IPv6 address.
<i>if_name</i>	If the next hop is a link-local address, the name of the interface used to reach it.
<i>metric</i>	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
<i>metric</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 | ospf | rip | ebgp | ibgp} value
```

Syntax Definitions

static	Configures the route preference of static routes.
ospf	Configures the route preference of OSPF3 routes.
rip	Configures the route preference of RIPng routes.
ebgp	Configures the route preference of external BGP routes.
ibgp	Configures the route preference of internal BGP routes.
<i>value</i>	Route preference value.

Defaults

parameter	default
static <i>value</i>	2
ospf <i>value</i>	110
rip <i>value</i>	120
ebgp <i>value</i>	190
ibgp <i>value</i>	200

Platforms Supported

OmniSwitch 10K, 6900

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 in the current release.

Examples

```
-> ipv6 route-pref ospf 20  
-> ipv6 route-pref rip 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 route-pref

Displays the configured route preference of a router.

MIB Objects

```
alaIprmRtPrefTable  
  alaIprmRtPrefLocal  
  alaIprmRtPrefStatic  
  alaIprmRtPrefOspf  
  alaIprmRtPrefRip  
  alaIprmRtPrefEbgp  
  alaIprmRtPrefIbgp
```

ipv6 virtual-source-mac

Configures the source MAC to be used for packets being sent from a VRRP instance.

`ipv6 virtual-source-mac {on | off }`

Syntax Definitions

on	The switch will use the VRRP virtual MAC address for all packets.
off	The switch will use the physical MAC address for all packets except VRRP advertisements.

Defaults

parameter	default
virtual-source-mac	off

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use this command to change which MAC address the switch will use as the source MAC when sending packets from a VRRP instance.
- This command has no affect on VRRP advertisements, the VRRP virtual MAC will always be used.

Examples

```
-> ipv6 virtual-source-mac on  
-> ipv6 virtual-source-mac off
```

Release History

Release 7.2.1; command was introduced.

Related Commands

[show ipv6 route-pref](#) Displays the configured route preference of a router.

MIB Objects

N/A

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

<i>ipv6_address</i>	IP address of the system to ping.
<i>hostname</i>	DNS name of the system to ping.
<i>if_name</i>	If the target is a link-local address, the name of the interface used to reach it.
<i>count</i>	Number of packets to be transmitted.
<i>size</i>	Size of the data portion of the packet sent for this ping, in bytes.
<i>seconds</i>	Interval, in seconds, at which ping packets are transmitted.

Defaults

parameter	default
<i>count</i>	6
<i>size</i>	8
interval <i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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 2001:db8:302::44
-> ping6 fe80::2d0:95ff:fe6a:f458 vlanif-23
```

Release History

Release 7.1.1; 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

tracert6

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.

tracert6 {*ipv6_address* | *hostname*} [*if_name*] [**max-hop** *hop_count*] [**dest-port** *port_number*] [**probe-count** *probe*] [**size** *size*] [**host-names** {*yes/no*}]

Syntax Definitions

<i>ipv6_address</i>	Destination IPv6 address. IPv6 address of the host whose route you want to trace.
<i>hostname</i>	DNS name of the host whose route you want to trace.
<i>if_name</i>	If the target is a link-local address, the name of the interface used to reach it.
<i>hop_count</i>	Maximum hop count for the trace.
<i>port</i>	Specific UDP port destination. By default, the destination port is chosen by tracert6.
<i>size</i>	The initial size for the probe packets. During the trace the packet size will be adjusted downward as path MTU information is received. The default and maximum value is 24,000 bytes with a minimum of 1,280 bytes.
<i>host-names</i>	Specify whether each hop should be shown as an IPv6 address or the host name corresponding to the address.
<i>probe</i>	Number of probes to be sent to a single hop.

Defaults

parameter	default
<i>hop_count</i>	32
<i>probe</i>	3
<i>host-names</i>	no

Platforms Supported

OmniSwitch 10K, 6900

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

```
-> tracert6 41EA:103::65C3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 virtual-source-mac](#)

Tests whether an IPv6 destination can be reached from the local switch.

MIB Objects

N/A

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 10K, 6900

Usage Guidelines

Use the ICMP table to monitor and troubleshoot the switch.

Examples

-> show ipv6 icmp statistics

Message	Current	Previous	Change
Received Total	857	0	857
Errors	0	0	0
Destination Unreachable	0	0	0
Packet Too Big	0	0	0
Time Exceeded	0	0	0
Parameter Problems	0	0	0
Echo Requests	0	0	0
Echo Replies	0	0	0
Group Membership Queries	0	0	0
Group Membership Responses	0	0	0
Group Membership Reductions	0	0	0
Router Solicitations	9	0	9
Router Advertisements	847	0	847
Neighbor Solicitations	1	0	1
Neighbor Advertisements	0	0	0
Redirects	0	0	0
Administratively Prohibited	0	0	0
Sent Total	18	0	18
Errors	0	0	0
Destination Unreachable	0	0	0
Packet Too Big	0	0	0
Time Exceeded	0	0	0
Parameter Problems	0	0	0
Echo Requests	0	0	0
Echo Replies	0	0	0
Group Membership Queries	0	0	0
Group Membership Responses	11	0	11
Group Membership Reductions	0	0	0
Router Solicitations	3	0	3

Router Advertisements	0	0	0
Neighbor Solicitations	4	0	4
Neighbor Advertisements	0	0	0
Redirects	0	0	0
Administratively Prohibited	0	0	0

output definitions

Total	Total number of ICMPv6 messages the switch received or attempted to send.
Errors	Number of ICMPv6 messages the switch sent or received but was unable to process because of ICMPv6-specific errors (bad checksums, bad length, etc.).
Destination Unreachable	Number of Destination Unreachable messages that were sent or received by the switch.
Packet Too Big	Number of Packet Too Big messages 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.
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.
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.
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.

Release History

Release 7.1.1; 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 10K, 6900

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		
tunnel_6to4	2002:d423:2323::35/64	Active	6to4 Tunnel
	2002:d423:2323::/64		
v6if-tunnel-137	fe80::2d0:95ff:fe12:f470/64	Disabled	Tunnel 2
	137:35:35::35/64		
	137:35:35::/64		
loopback	::1/128	Active	loopback
		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 tunnel_6to4
tunnel_6to4
  IPv6 interface index           = 16777216(0x
  Administrative status         = Disabled
  Operational status             = Inactive
  Link-local address(es):
  Global unicast address(es):
  Anycast address(es):
  VRRP address(es):
  Joined group addresses:
    ff02::1
  Maximum Transfer Unit (MTU)   = 1280
  Neighbor reachable time (sec) = 465
  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)       = 0
  RA retransmit timer (ms)     = 0
  RA default lifetime (sec)    = 1800
  RA hop limit                  = 64
  RA send MTU option           = No
  RA clock skew (sec)          = 600

```

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).
Link-local address	Link-local address assigned to the interface.
Global unicast address(es)	Global unicast address(es) assigned to the interface.
Anycast address(es)	The anycast addresses assigned to the interface.
VRRP address(es)	Addresses assigned to the interface because a VRRP virtual router is active. If (accept) is present, the switch will accept packets destined to the address. If not present, any such packets will be discarded.
Joined group address(es)	Addresses of the multicast groups that this interface has joined.
Maximum Transfer Unit	Interface MTU value.
Neighbor reachable time (sec)	The amount of time that a neighbor reached through this interface will remain in the reachable state.
Base reachable time (sec)	The base reachable time used to calculate the current neighbor reachable time.
Retransmit timer (ms)	The interval at which neighbour solicitations will be retransmitted during the neighbor discovery process.
DAD transmits	The number of neighbour solicitations that will be sent as part of the Duplicate Address Detection process.

output definitions (continued)

Send Router Advertisements	Indicates if the router sends periodic router advertisements and responds to router solicitations on the interface.
Maximum RA interval (sec)	Maximum time between the transmission of unsolicited router advertisements over the interface.
Minimum RA interval (sec)	Minimum time between the transmission of unsolicited router advertisements over the interface (0.33 * Maximum RA Interval).
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 (sec)	The value placed in the router lifetime field in the router advertisements sent over this interface.
RA hop limit	The value placed in the current hop limit field in the router advertisements sent over this interface.
RA Send MTU option	Specifies whether the MTU option is included in the router advertisements sent over this interface.
RA clock skew (sec)	The clock skew allowed for router advertisements on this interface.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 address	Configures an IPv6 address on a VLAN, configured tunnel, or a 6to4 tunnel.
ipv6 interface	Configures an IPv6 interface on a VLAN.

MIB Objects

```

ipv6InterfaceTable
  ipv6AdminStatus
  ipv6IfOperStatus
  ipv6PhysicalAddress
  ipv6InterfaceAddress
  ipv6AddrAddress
  ipv6AddrAddressPfxLength
  ipv6Address
  ipv6AddressPrefix

```

```
alaIPv6InterfaceTable
  alaIPv6InterfaceName
  alaIPv6InterfaceAddress
  alaIPv6InterfaceAddressPrefixLength
  alaIPv6InterfaceAddressVRRPFlag
  alaIPv6MulticastGroupAddress
  alaIPv6InterfaceMtu
  alaIPv6InterfaceReachableTime
  alaIPv6InterfaceBaseReachableTime
  alaIPv6InterfaceRetransTimer
  alaIPv6InterfaceDADTransmits
  alaIPv6InterfaceSendRouterAdvertisements
  alaIPv6InterfaceMaxRtrAdvInterval
  alaIPv6InterfaceMinRtrAdvInterval
  alaIPv6InterfaceAdvManagedFlag
  alaIPv6InterfaceAdvOtherConfigFlag
  alaIPv6InterfaceAdvReachableTime
  alaIPv6InterfaceAdvRetransTimer
  alaIPv6InterfaceClockSkew
  alaIPv6InterfaceAdvHopLimit
  alaIPv6InterfaceAdvSendMtu
  alaIPv6InterfaceAdvDefaultLifetime
```

show ipv6 pmtu table

Displays the IPv6 Path MTU Table.

show ipv6 pmtu table

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[ipv6 pmtu-lifetime](#) Configures the minimum lifetime for entries in the path MTU Table.

MIB Objects

```
alaIPv6ConfigTable
  alaIPv6PMTUDest
  alaIPv6PMTUexpire
```

show ipv6 neighbors

Displays IPv6 Neighbor Table.

show ipv6 neighbors [*ipv6_prefix/prefix_length* | *if_name* | **hw** *hardware_address* | **static**]

Syntax Definitions

<i>ipv6_prefix/prefix_length</i>	IPv6 prefix. Restricts the display to those neighbors starting with the specified prefix.
<i>if_name</i>	Interface name. Restricts the display to those neighbors reached through the specified interface.
<i>hardware_address</i>	MAC address. Restricts the display to the specified MAC address.
static	Restricts display to statically configured neighbors.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you do not specify an option (e.g., *if_name*), all IPv6 neighbors are displayed.

Examples

```
-> show ipv6 neighbors
Total 2 neighbors
```

```
IPv6 Address           Hardware Address  Reachability Lifetime      Port   Interface
-----+-----+-----+-----+-----+-----
2001:db8:39::11      0a:3f:1e:ac:7b:38 Unconfirmed 39s           1/ 1   vlan-41
fe80::83f:1eff:feac:7b38 0a:3f:1e:ac:7b:38 Confirmed 8m 21s       1/ 1   vlan-41
```

output definitions

IPv6 Address	The neighbor's IPv6 address.
Hardware Address	The MAC address corresponding to the IPv6 address.
Reachability	The neighbor's reachability: <ul style="list-style-type: none"> • Incomplete • Confirmed • Unconfirmed
Lifetime	The time the entry will remain in its current state.
Port	The port used to reach the neighbor.
Interface	The neighbor's interface name (e.g., <i>vlan_1</i>)

Release History

Release 7.1.1; 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 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

N/A

Examples

-> show ipv6 prefixes

Legend: Flags: A = Autonomous Address Configuration, L = OnLink

Name	IPv6 Address/Prefix Length	Valid Lifetime	Preferred Lifetime	Flags	Source
vlan 955	212:95:5::/64	2592000	604800	LA	dynamic
vlan 1002	195:35::/64	2592000	604800	LA	dynamic
6to4tunnel	2002:d423:2323::/64	2592000	604800	LA	dynamic
tunnel 2	137:35:35::/64	2592000	604800	LA	dynamic

output definitions

Name	The interface name. This is usually the VLAN on which the interface is configured.
IPv6 Address/Prefix Length	The IPv6 prefix and prefix length for a Router Advertisement Prefix Option.
Valid Lifetime	Length of time, in seconds, that this prefix will remain valid (i.e., time until deprecation). A value of 4,294,967,295 represents infinity.
Preferred Lifetime	Length of time, in seconds, that this prefix will remain preferred (i.e. time until deprecation). A value of 4,294,967,295 represents infinity.
Flags	L - Prefix can be used for onlink determination. A - Prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
Source	config - Prefix has been configured by management. dynamic - Router Advertisements are using interface prefixes.

Release History

Release 7.1.1; 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 10K, 6900

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
::/0	2002:d468:8a89::137	v6if-6to4-137	18h 47m 26s	Static	UGS
137:35:35::/64	fe80::2d0:95ff:fe12:f470	v6if-tunnel-137	18h 51m 55s	Local	UC
195:35::/64	fe80::2d0:95ff:fe12:f470	v6if-to-eagle	18h 51m 55s	Local	UC
212:95:5::/64	fe80::2d0:95ff:fe12:f470	smbif-5	18h 51m 55s	Local	UC
2002::/16	2002:d423:2323::35	v6if-6to4-137	18h 51m 55s	Other	U

output definitions

Destination Prefix	IPv6 destination address and prefix.
Gateway Address	IPv6 address of the gateway used to reach the destination network.
Interface	The device the interface is using (e.g., VLAN 6to4tunnel); or loopback.
Age	Age of the entry. Entries less than 1 day old are displayed in hh:mm:ss format. Entries more than 1 day old are displayed in dd:hh format.
Protocol	Protocol by which the route was learned.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 static-route](#) Configures a static entry in the IPv6 route.

MIB Objects

```
IPv6RouteTable
  IPv6Routes
  IPv6RoutesPrefix
  IPV6RoutesStatic
alaIPv6StaticRouteTable
  alaIPv6StaticRouteEntry
```

show ipv6 route-pref

Displays the IPv6 routing preference of the router.

```
show ipv6 route-pref
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The IPv6 version of BGP is not supported in the current release.

Examples

```
-> show ipv6 route-pref
  Protocol      Route Preference Value
-----+-----
  Local         1
  Static        2
  OSPF          110
  RIP           120
  EBGP          190
  IBGP          200
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 route-pref](#) Configures the IPv6 route preference of a router.

show ipv6 router database

Displays a list of all routes (static and dynamic) that exist in the IPv6 router database. This database serves as a central repository where routes are first processed for redistribution and where duplicate routes are compared to determine the best route to use. If a route does not appear in the IPv6 router database list, then the switch does not know about it. In the case of dynamically learned routes, this could indicate that the route was never received by the switch.

show ipv6 router database [**protocol** *type* / **gateway** *ipv6_address* / **dest** *ipv6_prefix/prefix_length*]

Syntax Definitions

<i>type</i>	Routing protocol type (local, static, OSPF, RIP, or BGP).
gateway <i>ipv6_address</i>	IPv6 address of the next hop used to reach the destination IPv6 address.
<i>ipv6_prefix</i>	IPv6 network that is the destination of this static route.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask). (0...128).

Defaults

By default, all routes are displayed.

Platforms Supported

OmniSwitch 10K, 6900

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, OSPF, RIP, then BGP routes. As a result, a route that is known to the switch may not appear in the IP forwarding table if a duplicate route with a higher protocol precedence exists.
- A list of inactive static routes is also included in the **show ipv6 router database** output display. A route becomes inactive if the interface for its gateway goes down. Inactive routes are unable to get to their destination and further investigation is warranted to determine why their gateway is unavailable.
- Routes that appear as inactive are not included in the main IP router database listing. If an inactive route becomes active, however, it is removed from the inactive list and added to the active route list.

Examples

-> show ipv6 router database
 Legend: + indicates routes in use

Total IPRM IPv6 routes: 5

Destination/Prefix	Gateway Address	Interface	Protocol	Metric
::/0	2002:d468:8a89::137	v6if-6to4-137	Static	1
137:35:35::/64	fe80::2d0:95ff:fe12:f470	v6if-tunnel-137	OSPF	2
195:35::/64	fe80::2d0:95ff:fe12:f470	v6if-to-eagle	OSPF	2
212:95:5::/64	fe80::2d0:95ff:fe12:f470	smbif-5	Local	1
2002::/16	2002:d423:2323::35	v6if-6to4-137	Local	1

Inactive Static Routes:

VLAN	Destination/Prefix	Gateway Address	Metric
1510	212:95:5::/64	fe80::2d0:95ff:fe6a:f458	1

output definitions

Destination/Prefix	IPv6 destination address and prefix.
Gateway Address	IPv6 address of the gateway used to reach the destination network.
Interface	The device the interface is using (e.g., VLAN 6to4tunnel); or loopback.
Protocol	Protocol by which this IPv6 address was learned: LOCAL, STATIC, OSPF, RIP, BGP).
Metric	RIP metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.
VLAN	The VLAN on which the route was <i>learned</i> , not forwarded. Note that N/A appears in this field for static routes as they are not learned on a VLAN.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 routes](#) Displays the IPv6 Forwarding Table.

MIB Objects

N/A

show ipv6 tcp connections

Displays the TCP connections over the IPV6 table.

show ipv6 tcp connections

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

-> show ipv6 tcp connections

Local Address	Port	Remote Address	Port	State
2001:0000:0200::23	23	2001:0000:0400::143	1867	established
2001:0000:0200::23	8734	2001:0000:0200::19	8735	timeWait

output definitions

Local Address	The local IPV6 address for the TCP connection .
Port	The local port number of the TCP connection.
Remote Address	The remote IPV6 address for the TCP connection.
Port	The remote port number of the TCP connection.
State	The state of the TCP connection.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 tcp listeners](#)

Displays the TCP connections over the IPV6 listeners (endpoints awaiting a connection request).

MIB Objects

```
alaRipngInterfaceTable  
  alaRipngInterfaceStatus  
  alaRipngRouteTag  
  alaRipngInvalidTimer  
  alaRipngGarbageTimer  
  alaRipngHolddownTimer  
  alaRipngJitter  
  alaRipngTriggeredSends
```

show ipv6 tcp listeners

Displays the TCP connections over the IPV6 listeners (endpoints awaiting a connection request).

show ipv6 tcp listeners

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 tcp listeners
```

```
Local Address                               Port
-----+-----
::0                                         21
::0                                         23
::0                                         80
```

output definitions

Local Address	The local IPV6 address for this TCP listener. A value of ::0 indicates that the listener will accept a connection request sent to any of the switch's addresses.
Port	The local port number on which the listener is awaiting connection requests.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 tcp connections](#) Displays the TCP connections over the IPV6 table.

MIB Objects

```
alaRipngInterfaceTable
  alaRipngInterfaceStatus
```

```
alaRipngRouteTag  
laRipngInvalidTimer  
alaRipngGarbageTimer  
alaRipngHolddownTimer  
alaRipngJitter  
alaRipngTriggeredSends
```

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 10K, 6900

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
```

Message	Current	Previous	Change
-----+-----+-----+-----			
Packets received			
Total	66193	0	66193
Header errors	0	0	0
Too big	0	0	0
No route	0	0	0
Address errors	0	0	0
Unknown protocol	0	0	0
Truncated packets	0	0	0
Local discards	0	0	0
Delivered to users	969	0	969
Reassembly needed	0	0	0
Reassembly failed	0	0	0
Multicast packets	66191	0	66191
Packets sent			
Forwarded	0	0	0
Generated	23	0	23
Local discards	5	0	5
Fragmented	0	0	0
Fragmentation failed	0	0	0
Fragments generated	0	0	0
Multicast packets	34	0	34

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.
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 7.1.1; 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
```

show ipv6 tunnel configured

Displays IPv6 tunnel information and whether the 6to4 tunnel is enabled.

show ipv6 tunnel configured

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 tunnel configured
```

```
IPv6 6to4 tunnel: Enabled
```

```
Configured Tunnels:
```

Tunnel	IPv6 Address/Prefix Length	Source IPv4	Destination IPv4
1	2001:0000:0200::101/48	192.16.10.101	192.28.5.254
23	2001:0000:0200::102/48	192.15.10.102	10.27.105.25
v6if-tunnel-137	fe80::2d0:95ff:fe12:f470/64	212.35.35.35	212.104.138.137

output definitions

IPv6 6to4 tunnel	Indicates whether 6to4 tunneling is enabled or disabled on the switch.
Tunnel	Tunnel ID.
IPv6 Address/Prefix Length	IPv6 address associated with the tunnel.
Source IPv4	Source IPv4 address for the tunnel.
Destination IPv4	Destination IPv4 address for the tunnel.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 interface](#)

Configures an IPv6 interface on a VLAN or IPv6 tunnel.

MIB Objects

```
alaIPv6ConfigTunnelTable  
  alaIPv6Tunnel6to4  
  alaIPv6ConfigTunnelv4Source  
  alaIPv6ConfigTunnelv4Dest
```

show ipv6 tunnel 6to4

Displays IPv6 tunnel information and whether the 6to4 tunnel is enabled.

show ipv6 tunnel 6to4

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 tunnel 6to4
tunnel_6to4
  Status = Disabled
  IPv6 Address(es):
  Local IPv4 Address(es):
```

output definitions

Name	Indicates whether 6to4 tunneling is enabled or disabled on the switch.
Status	Tunnel ID.
IPv6 Address(es)	IPv6 address associated with the tunnel.
Local IPv4 Addresses(es)	Source IPv4 address for the tunnel.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 interface](#) Configures an IPv6 interface on a VLAN or IPv6 tunnel.

MIB Objects

```
alaIPv6ConfigTunnelTable
  alaIPv6Tunnel6to4
  alaIPv6ConfigTunnelv4Source
  alaIPv6ConfigTunnelv4Dest
```

show ipv6 udp ports

Displays UDP Over IPv6 Listener Table. This table contains information about UDP/IPv6 endpoints.

show ipv6 udp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show ipv6 routes](#) 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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 information
Default hop limit                = 64
Path MTU entry minimum lifetime (min) = 10
Neighbor stale lifetime (min)    = 10
Local Unicast Global ID          = 70:3302:a472
```

output definitions

Default hop limit	The value placed in the hop limit field in router advertisements
Path MTU entry minimum lifetime	Minimum lifetime for entries in the path MTU.
Neighbor stale lifetime	Minimum lifetime for neighbor entries in the stale state.
Local Unicast Global ID	The default global ID value used in unique local unicast addresses. "none" if a global ID has not been configured.

Release History

Release 7.1.1; 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.
ipv6 address global-id	Configures the default global ID for unique local unicast addresses

MIB Objects

ipv6MibObjects

Ipv6DefaultHopLimit

alaIPv6ConfigTable

alaIPv6PMTUMinLifetime

alaIPv6NeighborTable

 alaIPv6NeighborStaleLifetime

ipv6 redist

Controls the conditions for redistributing IPv6 routes between different protocols.

```
ipv6 redist {local | static | rip | ospf | isis | bgp} into {rip | ospf | isis | bgp} route-map route-map-name
[admin-state {enable | disable}]
```

```
no ipv6 redist {local | static | ospf | isis | bgp} into {rip | ospf | isis | bgp} [route-map route-map-name]
```

Syntax Definitions

local	Redistributes local IPv6 routes.
static	Redistributes static IPv6 routes.
rip	Specifies RIP as the source or destination (into) protocol.
ospf	Specifies OSPF as the source or destination (into) protocol.
bgp	This parameter is currently not supported.
isis	This parameter is currently not supported.
<i>route-map-name</i>	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 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a route map redistribution configuration. Note that if a route map name is not specified, all route maps associated with the redistribution configuration are removed.
- The source and destination protocols must be loaded and enabled before redistribution occurs.
- The IPv6 version of BGP is not supported in the current release.
- 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 10K Network Configuration Guide* for more information about how to create a route map.

Examples

```
-> ipv6 redist rip into ospf route-map rip-to-ospf1
-> ipv6 redist rip into ospf route-map rip-to-ospf2
-> no ipv6 redist rip into ospf route-map rip-to-ospf2
-> ipv6 redist local into rip route-map local-to-rip
-> ipv6 redist local into rip route-map local-to-rip disable
```

Release History

Release 7.1.1; 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 10K, 6900

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 7.1.1; 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

<i>access-list-name</i>	Name of the IPv6 access list (up to 20 characters).
<i>address/prefixLen</i>	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 10K, 6900

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 7.1.1; 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 | ospf | bgp]
```

Syntax Definitions

rip	Displays the route map redistribution configurations that specify RIP as the destination (into) protocol.
ospf	Displays the route map redistribution configurations that specify OSPF as the destination (into) protocol.
bgp	This parameter is not supported.

Defaults

By default all route map redistribution configurations are shown.

Platforms Supported

OmniSwitch 10K, 6900

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 in the current release.

Release History

Release 7.1.1; command was introduced.

Examples

```
-> show ipv6 redist
```

Source Protocol	Destination Protocol	Status	Route Map
localIPv6	RIPng	Enabled	ipv6rm
RIPng	OSPFv3	Enabled	ipv6rm

```
-> show ipv6 redist ospf
```

Source Protocol	Destination Protocol	Status	Route Map
RIPng	OSPFv3	Enabled	ipv6rm

output definitions

Source Protocol	The protocol from which the routes are learned.
Destination Protocol	The protocol into which the source protocol routes are redistributed..
Status	The administrative status (Enabled or Disabled) of the route map redistribution configuration.
Route Map	The name of the route map that is applied with this redistribution configuration.

Related Commands

ipv6 redist Controls the conditions for redistributing IPv6 routes between different protocols.

MIB Objects

```
alaRouteMapRedistProtoTable  
  alaRouteMapRedistSrcProtoId  
  alaRouteMapRedistDestProtoId  
  alaRouteMapRedistRouteMapIndex  
  alaRouteMapRedistStatus  
  alaRouteMapRedistAddressType  
  alaRouteMapRedistRowStatus
```

show ipv6 access-list

Displays the contents of the specified IPv6 access list.

show ip access-list [*access-list-name*]

Syntax Definitions

access-list-name Name of the IPv6 access list.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 /
Name  Prefix Length  Effect  Redistribution
-----+-----+-----+-----
al_3  128::/64         permit  all-subnets
al_4  124::/64         permit  no-subnets
```

```
-> show ipv6 access-list 4
      Address /
Name  Prefix Length  Effect  Redistribution
-----+-----+-----+-----
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 7.1.1; 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 10K, 6900

Usage Guidelines

- RIPng will support a maximum of 1,000 routes.
- RIPng will support a maximum of 20 interfaces.
- Use the [ipv6 rip admin-state](#) command to enable RIPng on the switch.

Examples

```
-> ipv6 load rip
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip admin-state	Enables/disables RIPng routing on the switch.
show ipv6 rip	Displays RIPng status and general configuration parameters.

MIB Objects

```
alaDrcTmConfig  
  alaDrcTmIPRipngStatus
```

ipv6 rip admin-state

Enables or disables RIPng on the switch.

ipv6 rip admin-state {enable | disable}

Syntax Definitions

N/A

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

RIPng must be loaded on the switch ([ipv6 load rip](#)) to enable RIP on the switch.

Examples

```
-> ipv6 rip admin-state enable
```

Release History

Release 7.1.1; 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
<i>seconds</i>	180

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This timer is reset each time a routing update is received.

Examples

```
-> ipv6 rip invalid-timer 300
```

Release History

Release 7.1.1; 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
<i>seconds</i>	120

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the [ipv6 rip invalid-timer](#) command to set the Invalid Timer Value.

Examples

```
-> ipv6 rip garbage-timer 180
```

Release History

Release 7.1.1; 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
<i>seconds</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>value</i>	5

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>seconds</i>	30

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

- By default, a RIPng interface is created in the enabled state.
- Routing is enabled on a VLAN when you create a router port. However, to enable RIPng routing, you must also configure and enable a RIPng routing interface on the VLAN's IP router port. For more information on VLANs and router ports, see [Chapter 4, "VLAN Management Commands"](#).
- RIPng will support a maximum of 20 interfaces.

Examples

```
-> ipv6 rip interface Test_Lab
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 redist	Loads RIPng into memory.
ipv6 rip admin-state	Enables or disables RIPng on the switch.
ipv6 rip interface rcv-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
<i>value</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

RIPng must be loaded ([ipv6 load rip](#)) and enabled ([ipv6 rip admin-state](#)) on the switch to send or receive packets on the interface.

Examples

```
-> ipv6 rip interface Test_Lab recv-status disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 redist](#) Loads RIPng into memory.

[ipv6 rip admin-state](#) 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 10K, 6900

Usage Guidelines

RIPng must be loaded ([ipv6 load rip](#)) and enabled ([ipv6 rip admin-state](#)) on the switch to send or receive packets on the interface.

Examples

```
-> ipv6 rip interface Test_Lab send-status enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 redist](#) Loads RIPng into memory.

[ipv6 rip admin-state](#) 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

<i>if_name</i>	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 10K, 6900

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 7.1.1; 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 10K, 6900

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. 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 7.1.1; command was introduced.

Related Commands

ipv6 rip admin-state	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 10K, 6900

Usage Guidelines

If you do not specify an interface, all IPv6 RIP interfaces are displayed.

Examples

```
-> show ipv6 rip interface
```

Interface Name	Status	Packets		Metric
		Recvd	Sent	
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 7.1.1; command was introduced.

Related Commands

ipv6 rip interface	IPv6 interface name.
ipv6 rip admin-state	Enables or disables RIPng routing on the switch.
ipv6 rip interface rcv-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_address*]

Syntax Definitions

ipv6_address IPv6 address of the peer.

Defaults

N/A.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you do not specify a peer, all IPv6 RIP peers are displayed.

Examples

```
-> show ipv6 peer
```

Address	Seen on Interface	Packets Recv	Last 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 7.1.1; 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.
<i>ipv6_addr</i>	IPv6 address.
<i>ipv6_prefix/prefix length</i>	IPv6 address and prefix/prefix length.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
```

15 IPsec commands

IPsec is a suite of protocols for securing IPv6 communications by authenticating and/or encrypting each IPv6 packet in a data stream. IPsec provides security services such as Encrypting traffic, Integrity validation, Authenticating the peers, and Anti-replay.

IPsec protocols operate at network layer using appropriate security protocols, cryptographic algorithms, and cryptographic keys. The security services are provided through use of two security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

There are two modes of IPsec operation: transport mode and tunnel mode. In transport mode, only the data you transfer (payload) in the IPv6 packet is encrypted and/or authenticated and only the payloads that are originated and destined between two intermediate systems are processed with IPsec. In tunnel mode, the entire IPv6 packet with both the data and the message headers is encrypted and/or authenticated. In tunnel mode, all the IPv6 packets that pass through the endpoints are processed by IPsec. The current implementation of IPsec supports only the transport mode.

Note. The current implementation of IPsec supports only IPv6.

The pre-configured Security Policy determines the traffic that is to be rendered with IPsec protection. A Security Association (SA) specifies the actual IPsec actions to be performed (e.g encryption using 3DES, authentication with HMAC-SHA1). A security association is bundle of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. Security Associations can be manually configured or negotiated through IKE. The current implementation of IPsec does not support the negotiation of SA through IKE and SAs need to be configured manually.

A summary of the available commands is listed here:

- [ipsec key](#)
- [ipsec security-key](#)
- [ipsec policy](#)
- [ipsec policy rule](#)
- [ipsec sa](#)
- [show ipsec policy](#)
- [show ipsec sa](#)
- [show ipsec key](#)
- [show ipsec ipv6 statistics](#)

ipsec key

Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

ipsec key *name* {**sa-authentication** | **sa-encryption**} [**encrypted**] *key*

no ipsec key *name* {**sa-authentication** | **sa-encryption**}

Syntax Definitions

<i>name</i>	The name of this key (maximum 20 characters).
sa-authentication	Indicates that the key value is used for Authentication Header.
sa-encryption	Indicates that the key value is used for Encapsulated Security Payload.
encrypted	Not user configured, used only by switch in config file.
<i>key</i>	Specifies the key value. The key value can be either in the hexadecimal format or as a string.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The *name* parameter must be same as the name of the manually configured SA that uses this SA authentication and encryption key.
- The length of the key value must match the value that is required by the encryption or authentication algorithm that uses the key. The required key length for the supported algorithm are as follows:

algorithm	key length
3des-cbc	192 bits
aes-cbc	128, 192, or 256 bits
hmac-md5	128 bits
hmac-sha1	160 bits
aes-xcbc-mac	128

- The combination of the key's name and type must be unique.
- The **encrypted** option is used when the key commands are written to the boot.cfg or other snapshot file. This option can not be specified by the user when entering CLI commands.

Examples

```
-> ipsec key sa_md5_in sa-authentication takd03c9@skL68L%
```

Release History

Release 7.1.1; command introduced.

Related Commands

- | | |
|--------------------------------|---|
| ipsec sa | Adds, modifies, or deletes a manually configured IPsec Security Association (SA). |
| show ipsec key | Displays the keys for the manually configured IPsec SA. |

MIB Objects

AlaIPsecKeyTable
 alaIPsecKeyName
 alaIPsecKeyType
 alaIPsecKeyEncrypted
 alaIPsecKey

ipsec security-key

Sets the master security key for the switch. The master security key is used to encrypt and decrypt the configured SA keys.

ipsec security-key [*old_key*] *new_key*

Syntax Definitions

<i>old_key</i>	The current master security key. The key can be specified either in the hexadecimal format or as a string.
<i>new_key</i>	The new key value. The key can be specified either in the hexadecimal format or as a string.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The *old_key* parameter must always be specified when you modify an existing key. Setting the key for first time does not require the *old_key*.
- If the value of the *old_key* is incorrect, the attempt to set a new key fails.
- While the SA keys can be configured without a master security key; the configured SA keys are written to the configuration file unencrypted, and a warning is logged.
- The security key must be 16 characters or 16 bytes if in hex form (32 hex digits).
- If the master security key is reset using **debug clear ipsec security key** command, the currently configured SA keys are deleted.

Examples

```
-> ipsec security-key "old key value ab" 0xa38d901bde77af091a2485ce0a14a8cc
```

Release History

Release 7.1.1; command introduced.

Related Commands

[ipsec key](#)

Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

MIB Objects

```
AlaIPsecSecurityKeyTable  
  alaIPsecSecurityKeyCurrent  
  alaIPsecSecurityKeyNew
```

ipsec policy

Adds, modifies, or removes a security policy.

ipsec policy *name* [**priority** *priority*] [**source** {*ipv6_address* [/*prefix_length*]}] [**port** *port*] [**destination** {*ipv6_address* [/*prefix_length*]}] [**port** *port*] [**protocol** {**any** | **icmp6** [**type** *type*]}] **tcp** | **udp** | **ospf** | **vrrp** | **number** *protocol*] [**in** | **out**] [**discard** | **ipsec** | **none**] [**description** *description*] [**admin-state** {**enable** | **disable**}]

no ipsec policy *name*

Syntax Definitions

<i>name</i>	The name for the policy
<i>priority</i>	The priority for the policy. Values may range from 1 to 1000. The lower the value, the higher the priority.
source <i>ipv6_address</i>	Specifies the source address of the IPv6 traffic that is covered by the policy.
source / <i>prefix_length</i>	Specifies the prefix length of the source address of the IPv6 traffic that is covered by the policy.
source <i>port</i>	Specifies the source port of the IPv6 traffic that is covered by the policy. The value 0 can be specified to match packets originated from any port.
destination <i>ipv6_address</i>	Specifies the destination address of the IPv6 traffic that is covered by the policy.
destination / <i>prefix-length</i>	Specifies the prefix length of the destination address of the IPv6 traffic that is covered by the policy.
destination <i>port</i>	Specifies the destination port of the IPv6 traffic that is covered by the policy. The value 0 can be specified to match packets destined to any port.
protocol	Specifies that the particular protocol specific traffic to be covered by the policy (Refer to the table in the “Usage Guidelines“ section below for various protocol options).
in	Specifies that the policy is applied to the inbound IPv6 traffic.
out	Specifies that the policy is applied to the outbound IPv6 traffic.
discard	Specifies the policy to discard the IPv6 packet, if it matches the criteria.
ipsec	Specifies the policy to send the IPv6 packet for IPsec processing, if it matches the criteria.
none	Specifies IPsec should not process the packet.
<i>description</i>	The detailed description of the policy.
admin-state enable	Administratively enables the policy.
admin-state disable	Administratively disables the policy.

Defaults

parameter	default
priority	100
<i>port</i>	0
any icmp6 tcp udp ospf vrrp number	any
icmp6 <i>type</i>	not present
discard ipsec none	ipsec
admin-state	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If two policies can cover the same traffic, the policy with the highest priority is applied. If two policies have the same priority, the one configured first has precedence.
- The following table lists the various **protocol** options in this command:

protocol
any
icmp6 [<i>type type</i>]
tcp
udp
ospf
vrrp
number <i>protocol</i>

The **any** option must be used to apply the policy to all protocol traffic. Otherwise, an upper-layer protocol (or protocol number) may be specified to restrict the policy to the specified protocol traffic. The optional *type* parameter of **icmp6** can also be specified to restrict the policy for certain type of ICMPv6 packets.

- If the **ipsec** option is specified this policy cannot be enabled until at least one rule has been defined. The policy rules specify that IPsec algorithms be applied to the traffic that matches the policy.

Examples

```
-> ipsec policy tcp_out source 2001:db8:3::12 destination 201:db8:4::a3e protocol
tcp out ipsec description "Outbound TCP traffic" admin-state disable
-> no ipsec policy tcp_out
```

Release History

Release 7.1.1; command introduced.

Related Commands

ipsec policy rule	Adds, modifies, or removes an IPsec rule for a security policy.
show ipsec policy	Displays information about the security policies.

MIB Objects

```
AlaIPsecSecurityPolicyTable
  alaIPsecSecurityPolicyName
  alaIPsecSecurityPolicyPriority
  alaIPsecSecurityPolicySource
  alaIPsecSecurityPolicySourceType
  alaIPsecSecurityPolicySourcePrefixLength
  alaIPsecSecurityPolicySourcePort
  alaIPsecSecurityPolicyDestination
  alaIPsecSecurityPolicyDestinationType
  alaIPsecSecurityPolicyDestinationPrefixLength
  alaIPsecSecurityPolicyDestinationPort
  alaIPsecSecurityPolicyULProtocol
  alaIPsecSecurityPolicyICMPv6Type
  alaIPsecSecurityPolicyDirection
  alaIPsecSecurityPolicyAction
  alaIPsecSecurityPolicyDescription
  alaIPsecSecurityPolicyAdminState
```

ipsec policy rule

Adds, modifies, or removes an IPsec rule for a security policy.

ipsec policy *name* **rule** *index* [**ah** | **esp**]

no ipsec policy *name*

Syntax Definitions

<i>name</i>	The name of the security policy created by using the ipsec policy command.
<i>index</i>	The index of this rule. Values may range from 1 to 10.
ah	Specifies that the rule requires the presence of an Authentication Header (AH).
esp	Specifies that the rule requires the presence of an Encrypted Security Payload header (ESP).

Defaults

N/A.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

You can use the *index* parameter to specify the order in which the multiple rules for the same security policy is applied to the original payload.

Examples

```
-> ipsec policy alucent rule 1 ah
-> no ipsec policy alucent
```

Release History

Release 7.1.1; command introduced.

Related Commands

[ipsec policy](#) Adds, modifies, or removes a security policy.

MIB Objects

```
AlaIPsecSecurityPolicyRuleTable  
  alaIPsecSecurityPolicyName  
  alaIPsecSecurityPolicyRuleIndex  
  alaIPsecSecurityPolicyRuleProtocol
```

ipsec sa

Adds, modifies, or deletes a manually configured IPsec Security Association (SA).

ipsec sa *name* {**esp** | **ah**} [**source** *ipv6_address*] [**destination** *ipv6_address*] [**spi** *spi*] [**encryption** {**null** | **3des-cbc** | **aes-cbc** [**key-size** *key_length*]}] [**authentication** {**none** | **hmac-md5** | **hmac-sha1** | **aes-xcbc-mac**}] [**description** *description*] [**admin-state** {**enable** | **disable**}]

no ipsec sa *name*

Syntax Definitions

<i>name</i>	The name assigned to this IPsec SA.
esp	Specifies the type of security association as ESP.
ah	Specifies the type of security association as AH.
source <i>ipv6_address</i>	Specifies the source address of the IPv6 traffic that is covered by the SA.
destination <i>ipv6_address</i>	Specifies the destination address of the IPv6 traffic that is covered by the SA.
<i>spi</i>	The Security Parameters Index (SPI) for the SA.
encryption	Specifies the encryption algorithm to be used for traffic covered by the SA. This parameter must be used only when the SA type is ESP.
<i>key_length</i>	key length for the specified encryption algorithm.
authentication	Specifies the authentication algorithm to be used for traffic covered by the SA.
<i>description</i>	The detailed description of the SA.
admin-state enable	Administratively enables the SA.
admin-state disable	Administratively disables the SA.

Defaults

parameter	Defaults
encryption	none
authentication	none
admin-state	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **encryption** parameter must be specified with the **none** option, if **ESP** is being used to verify integrity only.
- If **null** is specified as the option for **encryption**, an integrity algorithm must be specified using the **authentication** parameter.
- To override a default key length in an **encryption** algorithm, the key length must be specified after the protocol name. The key length supported for various algorithm are as follows:

encryption algorithm	key length (in bits)
aes-cbc	128(default), 192, and 256

- For AH SAs, one of the authentication algorithms such as aes-xcbc-mac, hmac-md5 or hmac-sha1 must be specified.

Examples

```
-> ipsec sa esp_in_1 esp source 2001:db8:3::13d destination 2001:db8:1::24 spi
10392 encryption aes-cbc authentication hmac-sha1
-> no ipsec sa esp_in_1
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show ipsec sa](#) Displays information about manually configured IPsec Security Associations.

MIB Objects

```
AlaIPsecSAConfigTable
  alaIPsecSAConfigName
  alaIPsecSAConfigType
  alaIPsecSAConfigSource
  alaIPsecSAConfigSourceType
  alaIPsecSAConfigDestination
  alaIPsecSAConfigDestinationType
  alaIPsecSAConfigSPI
  alaIPsecSAConfigEncryptionAlgorithm
  alaIPsecSAConfigEncryptionKeyLength
  alaIPsecSAConfigAuthenticationAlgorithm
  alaIPsecSAConfigDescription
  alaIPsecSAConfigAdminState
```

show ipsec policy

Displays information about the security policies.

show ipsec policy [*name*]

Syntax Definitions

name The policy name.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *name* parameter to display information about a specific security policy.

Examples

```
-> show ipsec policy
Name          Source-> Destination          Protocol  Direction  Action   State
-----+-----+-----+-----+-----+-----
ftp-in-drop   ::/0->2001:db8:3::13d        TCP       in         discard active
telnet-in-1   2001:db8::/48->2001:db8:1::24 TCP       in         ipsec   active
telnet-out-1  2001:db8:1::24->2001:db8::/48 TCP       out        ipsec   active
```

output definitions

Name	The name of the security policy.
Source -> Destination	Indicates the source and destination of traffic covered by this policy.
Protocol	Indicates the protocol traffic covered by this policy. The protocol name (TCP) or protocol number (80) is displayed in this field.
Direction	Indicates whether the policy has been applied to the incoming or outgoing traffic.
Action	Indicates the action to be taken on the traffic covered by this policy.
State	Indicates the operational state of this policy.

```
-> show ipsec policy telnet-out-1
Name          = telnet-out-1
Source        = 2001:db8:1::24
Destination   = 2001:db8::/48
Protocol      = TCP
Direction     = out
Action        = ipsec
State         = active
Rules:
```

1) esp

2) ah

Description:

Require AH and ESP headers on outgoing telnet traffic.

output definitions

Name	The name of the security policy.
Source	Indicates the source of the traffic covered by this policy.
Destination	Indicates the destination of the traffic covered by this policy.
Protocol	Indicates the protocol traffic covered by this policy. The protocol name (TCP) or protocol number (80) is displayed in this field.
Direction	Indicates whether the policy has been applied to the incoming or outgoing traffic.
Action	Indicates the action to be taken on the traffic covered by this policy.
State	Indicates the operational state of this policy.
Rules	Indicates the rules specified for this policy.
Description	The description for this policy.

Release History

Release 7.1.1; command introduced.

Related Commands

[ipsec policy](#) Adds, modifies, or removes a security policy.

MIB Objects

```
AlaIPsecSecurityPolicyTable
  alaIPsecSecurityPolicyName
  alaIPsecSecurityPolicySource
  alaIPsecSecurityPolicySourceType
  alaIPsecSecurityPolicySourcePrefixLength
  alaIPsecSecurityPolicySourcePort
  alaIPsecSecurityPolicyDestination
  alaIPsecSecurityPolicyDestinationType
  alaIPsecSecurityPolicyDestinationPrefixLength
  alaIPsecSecurityPolicyDestinationPort
  alaIPsecSecurityPolicyProtocol
  alaIPsecSecurityPolicyDirection
  alaIPsecSecurityPolicyAction
  alaIPsecSecurityPolicyOperationalState
  alaIPsecSecurityPolicyRuleIndex
  alaIPsecSecurityPolicyRuleProtocol
  alaIPsecSecurityPolicyDescription
```

show ipsec sa

Displays information about manually configured IPsec Security Associations.

```
show ipsec sa [name | esp | ah]
```

Syntax Definitions

<i>name</i>	The name of the Security Association.
esp	Restricts the display to ESP type SAs.
ah	Restricts the display to AH type SAs.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the *name* parameter to display the information about a specific SA.
- Use esp or ah option to display the information about their respective type SAs.

Examples

```
-> show ipsec sa
Name          Type  Source-> Destination[SPI]          State  Encryption
Authentication
-----+-----+-----+-----+-----+-----+-----+-----
telnet-in-esp ESP  2001:db8::/49->2001:db8:1::24    active aes-cbc(128)
hmac-shal
telnet-out-esp ESP  2001:db8:1::24->2001:db8::/48    active aes-cbc(128)
hmac-shal
```

output definitions

Name	The SA name.
Type	The SA type: AH or ESP.
Source -> Destination [SPI]	The traffic source, traffic destination, and SPI for this SA.
State	The operational state of this SA.
Encryption	The encryption algorithm used for this SA.
Authentication	The authentication algorithm in use for this SA.

```

-> show ipsec sa telnet-in-esp

Name           = telnet-in-esp
Type           = ESP
Source         = 2001:db8::/48
Destination    = 2001:db8:1::24
SPI            = 8920
Encryption     = aes-cbc(128)
Authentication = hmac-shal

State          = active
Description:
  Security association for traffic from 2001:db8::/48 to
  2001:db8:1::24.

```

output definitions

Name	The SA name.
Type	The SA type: AH or ESP.
Source	The traffic source for this SA.
Destination	The traffic destination for this SA.
SPI	The SA's SPI.
Encryption	The encryption algorithm used for this SA.
Authentication	The authentication algorithm used for this SA.
State	The operational state of this SA.
Description	The SA's description.

Release History

Release 7.1.1; command introduced.

Related Commands

[ipsec sa](#) Adds, modifies, or deletes a manually configured IPsec Security Association (SA).

MIB Objects

```

AlaIPsecSAConfigTable
  alaIPsecSAConfigName
  alaIPsecSAConfigType
  alaIPsecSAConfigSource
  alaIPsecSAConfigSourceType
  alaIPsecSAConfigDestination
  alaIPsecSAConfigDestinationType
  alaIPsecSAConfigSPI
  alaIPsecSAConfigOperationalState
  alaIPsecSAConfigEncryptionAlgorithm
  alaIPsecSAConfigEncryptionKeyLength
  alaIPsecSAConfigAuthenticationAlgorithm
  alaIPsecSAConfigAuthenticationKeyLength
  alaIPsecSAConfigDescription

```

show ipsec key

Displays the keys for the manually configured IPsec SA.

show ipsec key [sa-encryption | sa-authentication]

Syntax Definitions

sa-encryption Displays the encryption keys.
sa-authentication Displays the authentication keys.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The key values are not be displayed due to security reasons.

Examples

```
-> show ipsec key sa-encryption
Encryption Keys
Name                               Length (bits)
-----+-----
sa_1                               192
sa_2                               160
sa_3                               64

-> show ipsec key sa-authentication
Authentication Keys
Name                               Length (bits)
-----+-----
sa_1                               128
sa_5                               160
```

output definitions

Name	The name of the SA for which the key is used.
Length	The length of the key in bits.

Release History

Release 7.1.1; command introduced.

Related Commands

[ipsec key](#)

Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

MIB Objects

AlaIPsecKeyTable

 alaIPsecKeyName

 alaIPsecKey

show ipsec ipv6 statistics

Displays IPsec statistics.

show ipsec ipv6 statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
Inbound:
  Discarded                = 2787
  Policy violation         = 0
  Authentication Failure   = 0
  No SA found              = 0
Outbound:
  Discarded                = 5135
  No SA found              = 19
```

output definitions

Discarded	The number of incoming packets discarded because they matched a discard policy.
Policy violation	The number of incoming packets that don't have the IPsec protection required by a security policy.
Authentication Failure	Authentication of a packet failed.
No SA found	No SA found matching the information present in a packet.

Release History

Release 7.1.1; command introduced.

Related Commands

N/A

MIB Objects

AlaIPsecStatisticsTable

```
alaIPsecStatisticsInDiscarded  
alaIPsecStatisticsInPolicyViolation  
alaIPsecStatisticsInAHAuthenticationFail  
alaIPsecStatisticsInNoSA  
alaIPsecStatisticsOutDiscarded  
alaIPsecStatisticsOutPolicyViolation  
alaIPsecStatisticsOutNoSA
```

16 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 admin-state
ip rip interface
ip rip interface admin-state
ip rip interface metric
ip rip interface send-version
ip rip interface recv-version
ip rip interface ingress-filter
ip rip interface egress-filter
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 10K, 6900

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 admin-state** command to enable RIP on the switch.

Examples

```
-> ip load rip
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip admin-state

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 admin-state

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 admin-state {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 10K, 6900

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 admin-state enable
```

Release History

Release 7.1.1; 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 10K, 6900

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 admin-state](#) command.
- You can create a RIP interface even if an IP router interface has not been configured. However, RIP will not function unless an IP router interface is configured with the RIP interface.
- For more information on VLANs and router ports, see [Chapter 4, "VLAN Management Commands"](#).

Examples

```
-> ip rip interface rip-1
```

Release History

Release 7.1.1; 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 admin-state	Enables/disables RIP routing on the switch.
ip rip interface admin-state	Enables/disables a RIP interface.

MIB Objects

```
rip2IfConfTable  
  rip2IfConfAddress  
  rip2IfConfStatus
```

ip rip interface admin-state

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} admin-state {enable | disable}
```

Syntax Definitions

interface_name The name of the interface.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You must first create a RIP interface by using the [ip rip interface](#) command before enabling the interface.
- You can create a RIP interface even if an IP router interface has not been configured. However, RIP will not function unless an IP router interface is configured with the RIP interface.
- For more information on VLANs and router ports, see [Chapter 4, “VLAN Management Commands”](#).

Examples

```
-> ip rip interface rip-1 admin-state enable
```

Release History

Release 7.1.1; 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 admin-state

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
<i>value</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>interface_name</i>	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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

ip rip interface rcv-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

<i>interface_name</i>	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 10K, 6900

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 7.1.1; 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 interface ingress-filter

Assigns an ingress route map filter to the specified RIP interface. Received route advertisements are compared against ingress filters. When a prefix matches the corresponding filter, that prefix is accepted on the interface. When a prefix does not match the filter, the prefix is dropped as if it was never received.

ip rip interface {*interface_name*} **ingress-filter** {*filter_name*}

Syntax Definitions

interface_name The name of an existing RIP interface.
filter_name The name of an existing route-map filter.

Defaults

By default, no such filter is associated with the RIP interface.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- One route-map filter is configurable in each direction (ingress/egress) for each RIP interface.
- Configuring multiple filters in the same direction for a single RIP interface is not supported.

Examples

```
-> ip route-map ripfilter1 action permit
-> ip route-map ripfilter1 match ip-address 202.5.0.0/16 deny
-> ip rip interface vlan-100 Ingress-filter RipFilter1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface egress-filter Assigns an egress route map filter to a RIP interface.
show ip rip interface Displays RIP interface status and configuration.

MIB Objects

ip rip interface ingress-filter

Assigns an ingress route map filter to the specified RIP interface. Received route advertisements are compared against ingress filters. When a prefix matches the corresponding filter, that prefix is accepted on the interface. When a prefix does not match the filter, the prefix is dropped as if it was never received.

ip rip interface {*interface_name*} **ingress-filter** {*filter_name*}

Syntax Definitions

<i>interface_name</i>	The name of an existing RIP interface.
<i>filter_name</i>	The name of an existing route-map filter.

Defaults

By default, no such filter is associated with the RIP interface.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- One route-map filter is configurable in each direction (ingress/egress) for each RIP interface.
- Configuring multiple filters in the same direction for a single RIP interface is not supported.

Examples

```
-> ip route-map ripfilter1 action permit
-> ip route-map ripfilter1 match ip-address 202.5.0.0/16 deny
-> ip rip interface vlan-100 ingress-filter RipFilter1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface egress-filter	Assigns an egress route map filter to a RIP interface.
show ip rip interface	Displays RIP interface status and configuration.

MIB Objects

ip rip interface egress-filter

Assigns an egress route map filter to the specified RIP interface. Outbound route advertisements are compared against egress filters. When a prefix matches the corresponding filter, that prefix is sent on the interface. When a prefix does not match the filter, the prefix is dropped as if it did not exist in the RIP RIB.

```
ip rip interface {interface_name} egress-filter {filter_name}
```

Syntax Definitions

<i>interface_name</i>	The name of an existing RIP interface.
<i>filter_name</i>	The name of an existing route-map filter.

Defaults

By default, no such filter is associated with the RIP interface.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- One route-map filter is configurable in each direction (ingress/egress) for each RIP interface.
- Configuring multiple filters in the same direction for a single RIP interface is not supported.

Examples

```
-> ip route-map ripfilter1 action permit
-> ip route-map ripfilter1 match ip-address 202.5.0.0/16 deny
-> ip rip interface vlan-100 egress-filter RipFilter1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip interface ingress-filter	Assigns an ingress route map filter to a RIP interface.
show ip rip interface	Displays RIP interface status and configuration.

MIB Objects

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
<i>seconds</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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.

Examples

```
-> ip rip force-holddowntimer 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands**show ip rip**

Displays the RIP status and general configuration parameters (for example, 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 10K, 6900

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 7.1.1; 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
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Only RIPv2 supports route tags.

Examples

```
-> ip rip route-tag 0
```

Release History

Release 7.1.1; 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

<i>interface_name</i>	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 10K, 6900

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 7.1.1; 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

<i>interface_name</i>	The name of the interface.
<i>string</i>	16-byte text string.

Defaults

The default authentication string is a null string.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>seconds</i>	30

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>seconds</i>	180

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The invalid time interval value must be three times the update interval value.

Examples

```
-> ip rip invalid-timer 270
```

Release History

Release 7.1.1; 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
<i>seconds</i>	120

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>seconds</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

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.
Invalid interval	The RIP invalid timer value, in seconds.
Garbage interval	The RIP garbage timer value, in seconds.
Holddown interval	The hold-down time interval, in seconds.
Forced Hold-Down Timer	The forced hold-down time interval, in seconds.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip admin-state	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 10K, 6900

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 7.1.1; 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 10K, 6900

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).
Interface Config Receive-Version	Interface receive option (none, v1, v2, and both).
Interface Config Default Metric	Default redistribution metric.
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 7.1.1; 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 10K, 6900

Usage Guidelines

N/A

Examples

-> show ip rip peer

IP Address	Total Recvd	Bad Packets	Bad Routes	Version	Secs since 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 7.1.1; 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
```

17 BFD Commands

Bidirectional Forwarding Detection (BFD) is a hello protocol, which can be configured to interact with routing protocols for the detection of path failures and can reduce the convergence time in a network. BFD is supported with the BGP, OSPF, VRRP, and Static Routes.

When BFD is configured and enabled, BFD sessions are created and timers are negotiated between BFD neighbors. If a system does not receive a BFD control packet within the negotiated time interval, the neighbor system is considered down. Rapid failure detection notices are then sent to the routing protocol, which initiates a routing protocol recalculation. This process can reduce the time of convergence in a network.

BFD can be operated in two different modes: Asynchronous mode with Echo enabled and Echo-Only mode. Demand mode is not supported.

In Asynchronous mode, the systems continuously send BFD control packets between each other as part of a BFD session. If there are no packets received for a minimum time interval negotiated between the systems, then the neighbor system is considered down.

In Echo mode, a stream of BFD echo packets are transmitted in a forwarding path for which the neighboring system would loop the packets and send them back. If the number of packets transmitted is not echoed back, then the system is declared down. Echo mode can be operated along with Asynchronous mode.

MIB information for the BFD commands is as follows:

Filename: ALCATEL-IND1-BFD-MIB
Module: ALCATEL-IND-BFD-MIB

A summary of the available commands is listed here:

Global BFD commands	ip bfd admin-state ip bfd transmit ip bfd receive ip bfd multiplier ip bfd echo-interval ip bfd interface show ip bfd show ip bfd sessions show ip bfd sessions statistics
----------------------------	---

BFD Interface commands	ip bfd interface ip bfd interface admin-state ip bfd interface transmit ip bfd interface receive ip bfd interface multiplier ip ospf bfd-state ip bfd interface echo-interval show ip bfd interfaces
Commands to configure BFD supported protocols	ip ospf bfd-state ip ospf bfd-state all-interfaces ip ospf interface bfd-state ip ospf interface bfd-state drs-only ip ospf interface bfd-state all-neighbors ip bgp bfd-state ip bgp bfd-state all-neighbors ip bgp neighbor bfd-state vrrp bfd-state vrrp track address bfd-state ip static-route all bfd-state ip static-route bfd-state

ip bfd admin-state

Enables or disables the global BFD protocol status for the switch.

```
ip bfd admin-state {enable | disable}
```

Syntax Definitions

enable	Enables BFD.
disable	Disables BFD.

Defaults

By default, BFD is disabled for the switch.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Disabling BFD does not remove the existing BFD configuration from the switch.
- When BFD is disabled, all BFD functionality is disabled for the switch, but configuring BFD is still allowed.
- Configuring BFD global parameters is not allowed when BFD is enabled for the switch.

Examples

```
-> ip bfd admin-state enable  
-> ip bfd admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bfd](#) Displays the BFD global status and general configuration parameters.

MIB Objects

alaBfdGlobalAdminStatus

ip bfd transmit

Configures the global transmit time interval for BFD control packets. This command specifies the minimum amount of time BFD waits between each transmission of control packets.

ip bfd transmit *transmit_interval*

Syntax Definitions

transmit_interval The transmit time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
<i>transmit_interval</i>	300 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The transmit time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd transmit** command does not override the value set for the interface using the **ip bfd interface transmit** command.
- The global transmit time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd transmit 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|---|--|
| ip bfd interface transmit | Configures the transmit time interval for a specific BFD interface. |
| show ip bfd | Displays the BFD global status and general configuration parameters. |

MIB Objects

alaBfdGlobalTxInterval

ip bfd receive

Configures the global receive time interval for BFD control packets. This command specifies the minimum amount of time BFD waits to receive control packets before determining there is a problem.

ip bfd receive *receive_interval*

Syntax Definitions

receive_interval The receive time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
<i>receive_interval</i>	300 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The minimum receive time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd receive** command does not override the value set for the interface using the **ip bfd interface receive** command.
- The global receive time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd receive 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bfd interface receive** Configures the receive time interval for a specific BFD interface.
- show ip bfd** Displays the BFD global status and general configuration parameters.

MIB Objects

alaBfdGlobalRxInterval

ip bfd multiplier

Configures the global BFD detection time multiplier. This command specifies a number that is used to calculate the BFD detection time used in the asynchronous mode. The detection time value that is specified determines how long to wait before declaring that the BFD session is down.

ip bfd multiplier *num*

Syntax Definitions

num The detection time multiplier number. The valid range is 3–255.

Defaults

By default, the multiplier value is set to 3.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The global detection time multiplier is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd multiplier** command does not override the value set for the interface using the **ip bfd interface multiplier** command.
- The global detection time multiplier serves as the default multiplier value for a BFD interface. The default multiplier value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd multiplier 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface multiplier	Configures the detection time multiplier for a BFD interface.
show ip bfd	Displays the BFD global status and general configuration parameters.

MIB Objects

alaBfdGlobalDetectMult

ip bfd echo-interval

Configures the global BFD echo packet time interval. The echo function is available with the asynchronous mode. Echo packets are transmitted to BFD peers to see if they loop back to the peer from which they originated.

ip bfd echo-interval *echo_interval*

Syntax Definitions

echo_interval The echo time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
<i>echo_interval</i>	300 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The echo packet time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd echo-interval** command does not override the value set for the interface using the **ip bfd interface echo-interval** command.
- The global echo packet time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

Examples

```
-> ip bfd echo-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bfd interface echo-interval** Configures the echo packet time interval for a BFD interface.
- show ip bfd** Displays the BFD global status and general configuration parameters.

MIB Objects

alaBfdGlobalEchoRxInterval

ip bfd interface

Configures a BFD interface.

ip bfd interface *if_name*

no ip bfd interface *if_name*

Syntax Definitions

if_name The name of an existing IP interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a BFD interface.
- The interface name must be an existing IP interface name that is configured with an IP address.

Examples

```
-> ip bfd interface bfd-vlan-101  
-> no ip bfd interface bfd-vlan-101
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface admin-state	Configures the administrative status of a BFD interface.
show ip bfd interfaces	Displays the status and statistics of a BFD interface.
show ip bfd sessions	Displays the status and statistics of the BFD sessions.

MIB Objects

```
alaBfdIntfTable  
  alaBfdIntfAddrType  
  alaBfdIntfAddr  
  alaBfdIntfIndex
```

ip bfd interface admin-state

Enables or disables the administrative status of a BFD interface.

ip bfd interface *if_name* admin-state {enable | disable}

Syntax Definitions

<i>if_name</i>	The name of an existing BFD interface.
enable	Enables the BFD interface.
disable	Disables the BFD interface.

Defaults

By default, a BFD interface is disabled when it is created.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The BFD interface must be enabled to participate in the BFD protocol.

Examples

```
-> ip bfd interface bfd-vlan-101 admin-state enable
-> ip bfd interface bfd-vlan-101 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface	Creates a BFD interface.
show ip bfd interfaces	Displays the status and statistics of a BFD interface.
show ip bfd sessions	Displays the status and statistics of BFD sessions.

MIB Objects

```
alaBfdIntfTable
  alaBfdIntfAdminStatus
```

ip bfd interface transmit

Configures the transmit time interval for the BFD interface. This command specifies the minimum amount of time BFD waits between each transmission of control packets from the interface.

ip bfd interface *if_name* **transmit** *transmit_interval*

Syntax Definitions

<i>if_name</i>	The name of an existing BFD interface.
<i>transmit_interval</i>	The transmit time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
<i>transmit_interval</i>	300 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The global transmit time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface transmit time interval using the **ip bfd interface transmit** command does not change the global value configured with the **ip bfd transmit** command.

Examples

```
-> ip bfd interface bfd-vlan-101 transmit 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface	Creates a BFD interface.
ip bfd transmit	Configures a global BFD transmit time interval.
show ip bfd interfaces	Displays the status and statistics of a BFD interface.
show ip bfd sessions	Displays the status and statistics of the BFD sessions.

MIB Objects

```
alaBfdIntfTable  
  alaBfdIntfDesiredMinTxInterval
```

ip bfd interface receive

Configures the receive time interval for the BFD interface. This command specifies the minimum amount of time BFD waits to receive control packets on the interface before determining there is a problem.

ip bfd interface *if_name* **receive** *receive_interval*

Syntax Definitions

<i>if_name</i>	The name of an existing BFD interface.
<i>receive_interval</i>	The receive time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
<i>receive_interval</i>	300 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The global receive time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface transmit time interval using the **ip bfd interface receive** command does not change the global value configured with the **ip bfd receive** command.

Examples

```
-> ip bfd interface bfd-vlan-101 receive 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface	Creates a BFD interface.
ip bfd receive	Configures a global BFD receive time interval.
show ip bfd interfaces	Displays the BFD interface configuration table.
show ip bfd sessions	Displays the BFD interface configuration table.

MIB Objects

alaBfdIntfTable
alaBfdReqMinRxInterval

ip bfd interface multiplier

Configures the BFD interface detection time multiplier. This command specifies a number that is used to calculate the BFD detection time used in the asynchronous mode. When an interface stops receiving packets from a neighbor, the interface uses the detection time value to determine how long to wait before declaring that the BFD session is down.

ip bfd interface *if_name* **multiplier** *num*

Syntax Definitions

<i>if_name</i>	The name of an existing BFD interface.
<i>num</i>	The detection time multiplier number. The valid range is 3–255.

Defaults

By default, the multiplier value is set to 3.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The detection time between neighbors is calculated by multiplying the negotiated transmit time interval by the detection time multiplier.

Examples

```
-> ip bfd interface bfd-vlan-101 multiplier 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface	Creates a BFD interface.
show ip bfd interfaces	Displays the BFD interface configuration table.
show ip bfd sessions	Displays the BFD interface configuration table.

MIB Objects

alaBfdIntfTable
alaBfdIntfDetectMult

ip bfd interface echo-interval

Configures the echo time interval for the BFD interface. The echo function is available with the asynchronous mode. Echo packets are transmitted to BFD peers to see if they loop back to the peer from which they originated.

ip bfd interface *if_name* **echo-interval** *echo_interval*

Syntax Definitions

<i>if_name</i>	The name of an existing IP interface.
<i>echo_interval</i>	The echo time interval, in milliseconds. The valid range is 100–999.

Defaults

parameter	default
<i>echo_interval</i>	300 milliseconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The global echo time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface echo time interval using the **ip bfd interface echo-interval** command does not change the global value configured with the **ip bfd echo-interval** command.

Examples

```
-> ip bfd interface bfd-vlan-101 echo-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface	Creates a BFD interface.
ip bfd echo-interval	Configures a global BFD echo time interval.
show ip bfd interfaces	Displays the BFD interface configuration table.
show ip bfd sessions	Displays the BFD interface configuration table.

MIB Objects

```
alaBfdIntfTable
  alaBfdIntfReqMinEchoRxInterval
```

ip ospf bfd-state

Enables or disables the BFD status for the OSPF protocol.

```
ip ospf bfd-state {enable | disable}
```

Syntax Definitions

enable	Enables BFD Status.
disable	Disables BFD Status.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- All the status changes on the neighbors are received from the BFD level and the OSPF protocol acts based upon the BFD message.
- Whenever a neighbor goes down, OSPF will inform BFD to remove that neighbor from the BFD active list.

Examples

```
-> ip ospf bfd-state enable  
-> ip ospf bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip ospf bfd-state all-interfaces** Enables or disables BFD for all OSPF interfaces configured.
- ip ospf interface bfd-state** Enables or disables BFD for a specific OSPF interface.
- ip ospf interface bfd-state drs-only** Establishes BFD sessions only on neighbors in full state.
- ip ospf interface bfd-state all-neighbors** Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

MIB Objects

alaProtocolospf
alaOspfBfdStatus

ip ospf bfd-state all-interfaces

Enables or disables BFD for all OSPF interfaces in the switch configuration.

```
ip ospf bfd-state all-interfaces {enable | disable}
```

Syntax Definitions

enable	Enables BFD for all the OSPF interfaces.
disable	Disables BFD for all the OSPF interfaces.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf bfd-state all-interfaces enable  
-> ip ospf bfd-state all-interfaces disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf bfd-state	Enables or disables the BFD status for the OSPF protocol.
ip ospf interface bfd-state	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
ip ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

MIB Objects

```
alaProtocolospf  
  alaOspfBfdAllInterfaces
```

ip ospf interface bfd-state

Enables or disables BFD for a specific OSPF interface.

ip ospf interface *if_name* **bfd-state** {**enable** | **disable**}

Syntax Definitions

<i>if_name</i>	The name of an existing OSPF interface.
enable	Enables the OSPF interface.
disable	Disables the OSPF interface.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-state enable
-> ip ospf interface int2 bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf bfd-state	Enables or disables the BFD status for the OSPF protocol.
ip ospf bfd-state all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.
ip ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

MIB Objects

```
alaOspfIfAugEntry
  ospfIfIpAddress
  alaOspfIfBfdStatus
```

ip ospf interface bfd-state drs-only

Establishes BFD sessions only with neighbors that are in the full state.

ip ospf interface *if_name* **bfd-state drs-only**

Syntax Definitions

if_name The name of an existing OSPF interface.

Defaults

parameter	default
drs-only	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The specified OSPF interface must be enabled to interact with BFD.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-state drs-only
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface admin-state	Enables or disables the BFD status for OSPF protocol.
ip ospf bfd-state all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-state	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-state all-neighbors	Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

MIB Objects

```
alaOspfIfAugEntry  
  ospfIfIpAddress  
  alaOspfIfBfdDrsOnly
```

ip ospf interface bfd-state all-neighbors

Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

ip ospf interface *if_name* bfd-state all-neighbors {enable | disable }

Syntax Definitions

if_name The name of an existing OSPF interface.

Defaults

parameter	default
all-neighbors	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The specified OSPF interface must be enabled to interact with BFD.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

Examples

```
-> ip ospf interface int1 bfd-state all-neighbors enable
-> ip ospf interface int1 bfd-state all-neighbors disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd interface admin-state	Enables or disables the BFD status for OSPF protocol.
ip ospf bfd-state all-interfaces	Enables or disables BFD for all OSPF interfaces configured.
ip ospf interface bfd-state	Enables or disables BFD for a specific OSPF interface.
ip ospf interface bfd-state drs-only	Establishes BFD sessions only on neighbors in full state.

MIB Objects

```
alaOspfIfAugEntry
  ospfIfIpAddress
  alaOspfIfBfdDrsOnly
```

ip bgp bfd-state

Enables or disables BFD for the BGP protocol.

```
ip bgp bfd-state {enable | disable}
```

Syntax Definitions

enable	Enables BGP.
disable	Disables BGP.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- All the status changes on the neighbors are received from the BFD level and the BGP protocol acts based upon the BFD message.
- Whenever a neighbor goes down, BGP will inform BFD to remove that neighbor from the BFD active list.

Examples

```
-> ip bgp bfd-state enable  
-> ip bgp bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- [ip bgp bfd-state all-neighbors](#) Enables or disables BFD for all BGP neighbors.
- [ip bgp neighbor bfd-state](#) Enables or disables BFD for a specific neighbor.

MIB Objects

```
alaBgpGlobal  
alaBgpBfdStatus
```

ip bgp bfd-state all-neighbors

Enables or disables BFD for all BGP neighbors.

ip bgp bfd-state all-neighbors {enable | disable}

Syntax Definitions

enable	Enables BFD for all the BGP neighbors.
disable	Disables BFD for all the BGP neighbors.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The BFD status for BGP must be enabled before BGP can interact with BFD.

Examples

```
-> ip bgp bfd-state all-neighbors enable
-> ip bgp bfd-state all-neighbors disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp bfd-state	Enables or disables BGP with BFD protocol.
ip bgp neighbor bfd-state	Enables or disables the BFD for a specific BGP neighbor.

MIB Objects

```
alaBgpGlobal
  alaBgpBfdAllNeighbors
```

ip bgp neighbor bfd-state

Enables or disables BFD for a specific BGP neighbor.

```
ip bgp neighbor ipv4_address bfd-state {enable | disable}
```

Syntax Definitions

<i>ipv4_address</i>	The IP address of the BGP neighbor.
enable	Enables BGP neighbor.
disable	Disables BGP neighbor.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The BFD status for BGP must be enabled before BGP can interact with BFD.

Examples

```
-> ip bgp neighbor 135.10.10.2 bfd-state enable
-> ip bgp neighbor 135.10.10.2 bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp bfd-state	Enables or disables BGP with BFD protocol.
ip bgp bfd-state all-neighbors	Enables or disables BFD for all BGP neighbors.

MIB Objects

```
alaBgpPeerEntry
  alaBgpPeerName
  alaBgpPeerBfdStatus
alaBgpGlobal
  alaBgpBfdAllNeighbors
```

vrrp bfd-state

Enables or disables VRRP with the BFD protocol.

vrrp bfd-state {enable | disable}

Syntax Definitions

enable	Enables BFD for VRRP.
disable	Disables BFD for VRRP.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- BFD support for VRRP is done only for tracking policy configuration for a remote address.
- The BFD status for VRRP must be enabled before VRRP can interact with BFD.

Examples

```
-> vrrp bfd-state enable
-> vrrp bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[vrrp track address bfd-state](#) Enables or disable BFD for a specific tracking policy.

MIB Objects

```
alaVrrpConfig
  alaVrrpBfdStatus
```

vrrp track address bfd-state

Enables or disable BFD for a specific track policy.

```
vrrp track track_id address ipv4_address bfd-state {enable| disable}
```

Syntax Definitions

<i>track_id</i>	The VRRP track number.
<i>ipv4_address</i>	The remote IP address.
enable	Enables BFD.
disable	Disables BFD.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- BFD support for VRRP is done only for tracking policy configuration for a remote address.
- The BFD status for VRRP must be enabled before VRRP can interact with BFD.

Examples

```
-> vrrp track 2 address 10.1.1.1 bfd-state enable  
-> vrrp track 3 address 10.1.1.2 bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[vrrp bfd-state](#) Enables or disables VRRP with BFD protocol.

MIB Objects

```
alaVRRPConfig  
  alaVrrpTrackBfdStatus
```

show ip bfd

Displays the global BFD configuration table.

show ip bfd

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip bfd
BFD Version Number           = 1,
Admin Status                  = Enabled,
Desired Transmit Interval    = 300,
Minimum Receive Interval     = 300,
Detection Time Multiplier    = 3,
Minimum Echo Receive Interval = 300,
Applications Registered       = STATIC-ROUTING OSPF
```

output definitions

BFD Version Number	Refers to BFD version.
Admin Status	Refers to BFD global admin status.
Desired Transmit Interval	Refers to BFD global Tx interval.
Minimum Receive Interval	Refers to BFD global Rx interval.
Detection Time Multiplier	Refers to the BFD Detection Time multiplier number.
Minimum Echo Receive Interval	Refers to BFD echo Rx interval.
Applications Registered	Refers to applications registered to BFD.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bfd admin-state](#)

Configures BFD at global level.

[ip bfd interface](#)

Configures BFD at interface level.

MIB Objects

alaBfdIntfTable

alaBfdGlobalVersionNumber

alaBfdGlobalAdminStatus

alaBfdGlobalTxInterval

alaBfdGlobalRxInterval

alaBfdGlobalDetectMult

alaBfdGlobalEchoRxInterval

alaBfdGlobalProtocolApps

show ip bfd interfaces

Displays the BFD interface configuration table.

show ip bfd interfaces [*if_name*]

Syntax Definitions

if_name The name of the BFD interface.

Defaults

By default, the configuration for all BFD interfaces is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Enter an interface name to display information for a specific BFD interface.

Examples

```
-> show ip bfd interfaces
Interface  Admin    Tx      Min Rx   Min EchoRx Detect   OperStatus
Name      Status  Interval Interval Interval Interval Multiplier
-----+-----+-----+-----+-----+-----+-----
one       enabled  300     300     300     300     3         UP
two       enabled  300     300     300     300     3         UP
```

```
-> show ip bfd interfaces one
Interface Name           = one,
Interface IP Address     = 100.1.1.1,
Admin Status             = Enabled,
Desired Transmit Interval = 300,
Minimum Receive Interval = 300,
Detection Time Multiplier = 3,
Minimum Echo Receive Interval = 300,
Authentication Present   = No,
Oper Status              = UP
```

output definitions

Interface Name	Refers to BFD Interface name.
Admin status	Refers to BFD interface admin status.
Desired Transmit Interval	Refers to BFD interface Tx interval.
Minimum Receive Interval	Refers to BFD interface Rx interval.
Detection Time Multiplier	Refers to BFD interface Detection Time Multiplier.
Minimum Echo Receive Interval	Refers to BFD interface echo Rx interval.

output definitions (continued)

Authentication Present	Refers to availability of BFD message authentication on the BFD interface.
Oper Status	Refers to BFD interface operational status.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd admin-state	Configures BFD at global level.
ip bfd interface	Configures BFD at interface level.

MIB Objects

```
alaBfdIntfTable
  alaBfdIntfIfName
  alaBfdIntfAddr
  alabfdIntfAdminStatus
  alaBfdIntfDesiredMinTxInterval
  alaBfdIntfReqMinRxInterval
  alaBfdIntfDetectMult
  alaBfdIntfReqMinEchoRxInterval
  alaBfdIntfAuthPresFlag
  alaBfdIntfOperStatus
```

show ip bfd sessions

Displays all the BFD sessions for the switch.

show ip bfd sessions [*session_num*] [*slot slot_num*]

Syntax Definitions

num The BFD session number. Valid range is 1–1024.

slot The current slot position used by the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip bfd sessions
Local   Interface Neighbor   State Remote Negotiated Negotiated Session
Discr   Name      Address    Discr   Discr  Rx Interval Tx Interval Type
-----+-----+-----+-----+-----+-----+-----+-----
1       one      100.1.1.10 UP      0      0          0          ECHO
2       one      101.1.1.11 UP      10     300       300       ASYNC
```

```
-> show ip bfd sessions slot 1
Local   Interface Neighbor   State Remote Negotiated Negotiated EchoRx
Discr   Name      Address    Discr   Discr  Rx Interval Tx Interval
-----+-----+-----+-----+-----+-----+-----+-----
1       one      100.1.1.10 UP      0      0          0          300
```

```
-> show ip bfd sessions 1
Local discriminator           = 1,
Neighbor IP Address          = 100.1.1.10,
Requested Session Type       = ECHO,
Interface IP Address         = 100.1.1.1,
Source UDP Port              = 49152,
State                        = UP,
Session Operating Mode       = ECHO only,
Remote discriminator         = 0,
Negotiated Tx interval       = 0,
Negotiated Rx interval       = 0,
Echo Rx interval             = 300,
Multiplier                   = 3,
Applications Registered:     = STATIC-ROUTING
```

output definitions

Local discriminator	The local discriminator.
Neighbor IP address	The IP address of the BFD neighbor.
Requested Session Type	The bit map of the session type that is requested. .
Interface IP address	The IP address of the outgoing BFD interface for this session.
Source UDP Port	The unique source UDP port used to send BFD packets for this session.
State	The state of the BFD session.
Session Operating Mode	The current operating mode of the BFD session.
Remote discriminator	The remote discriminator.
Negotiated Tx interval	The negotiated transmit interval.
Negotiated Rx interval	The negotiated receive interval.
Echo Rx interval	The Echo packet receive interval.
Detection Time Multiplier	The BFD Detection Time multiplier number.
Applications Registered	The bit map object of applications that are registered with this BFD session.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bfd admin-state	Configures BFD at global level.
ip bfd interface	Configures BFD at interface level.
show ip bfd sessions statistics	Displays the statistics for all BFD sessions.

MIB Objects

```

alaBfdSessTable
  alaBfdSessDiscriminator
  alaBfdSessNeighborAddr
  alaBfdSessSessionType
  alaBfdSessIfIndex
  alaBfdSessUdpPort
  alaBfdSessState
  alaBfdSessOperMode
  alaBfdSessDiscriminator
  alaBfdSessNegotiatedTxInterval
  alaBfdSessNegotiatedRxInterval
  alaBfdSessEchoRxInterval
  alaBfdSessDetectMult
  alaBfdSessProtocolApps

```

show ip bfd sessions statistics

Displays the statistics for all BFD sessions, a specific session or a specific slot.

show ip bfd sessions statistics *session_num*

Syntax Definitions

session_num The BFD session number. Valid range is 1–1024.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip bfd sessions statistics
Local      Neighbor      Tx      Rx      Echo Tx      Last Down      Up
Discr      Address      Packets  Packets  Packets      Diag Code      Count
-----+-----+-----+-----+-----+-----+-----
1      100.1.1.10      0      0      5772      0      1
2      101.1.1.11      5242     5241     0      0      1
```

```
-> show ip bfd sessions statistics 1
Tx packet counter      = 0,
Rx packet counter      = 0,
Tx Echo packet counter = 5772,
Rx Echo packet counter = 5774,
Session Up Time        = 6160400,
Session Down Time      = 0,
Last Down Diagnostic Code = 0,
Session Up Count       = 1
```

output definitions

Local discriminator	The local discriminator.
Neighbor address	The IP address of the BFD neighbor.
Tx Packets	Number of BFD Control packets transmitted on this session.
Rx Packets	Number of BFD Control packets received on this session.
Echo Tx Packets	Number of BFD Echo packets transmitted on this session.
Last Down Diagnostic Code	Diagnostic code for last session down event
Up Count	Number of times the session has moved to an UP state since the system was last reset or initialized.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bfd Displays the global BFD configuration table.
show ip bfd sessions Displays all BFD sessions.

MIB Objects

```
alaBfdSessPerfTable  
  alaBfdSessDiscriminator  
  alaBfdSessNeighborAddr  
  alaBfdSessPerfPktOut  
  alaBfdSessPerfPktIn  
  alaBfdSessPerfEchoOut  
  alaBfdSessPerfEchoIn  
  alaBfdSessPerfLastCommLostDiag  
  alaBfdSessPerfSessUpCount
```

ip static-route all bfd-state

Enables BFD for all static routes.

ip static-route all bfd-state {enable| disable}

Syntax Definitions

enable	Enables BFD.
disable	Disables BFD.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When there are static route configured in the switch, BFD is enabled to track the gateway.
- If the route is not reachable, it will be moved to the inactive database.

Examples

```
-> ip static-route all bfd-state enable  
-> ip static-route all bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIprmConfig  
alaIprmStaticallbfd
```

ip static-route bfd-state

Enables or disables BFD for a specific static route.

```
ip static-route ipv4_prefix/pfx_length gateway ipv4_host_address bfd-state {enable| disable}
```

Syntax Definitions

<i>ipv4_prefix</i>	The destination IP address.
<i>pfx_length</i>	The prefix length for the destination IP address.
gateway <i>ipv4_host_address</i>	The gateway IP address.
enable	Enables BFD.
disable	Disables BFD.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

BFD is enabled to track the gateway of static routes.

Examples

```
-> ip static-route 192.100.1.0/24 gateway 100.1.1.10 bfd-state enable
-> ip static-route 192.100.1.0/24 gateway 100.1.1.10 bfd-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip static-route all bfd-state](#) Enables BFD for all static routes.

MIB Objects

```
alaIprmStaticRouteEntry
  alaIprmStaticRouteDest
  alaIprmStaticRouteMask
  alaIprmStaticRouteNextHop
  alaIprmStaticRouteBfdStatus
```

18 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 (the 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. These CLI commands are applicable for all VRF instances.

MIB information for DHCP Relay commands is as follows:

Filename: AlcatelIND1UDPRelay.MIB
Module: ALCATEL-IND1-UDP-RELAY-MIB

A summary of the available commands is listed here.

ip helper address
ip helper vlan address
ip helper standard
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 boot-up
ip helper boot-up enable
ip udp relay port
ip udp relay service
ip udp relay service vlan
show ip helper
show ip helper statistics
show ip udp relay
show ip udp relay statistics
no ip helper statistics
ip udp relay no statistics

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*

no ip helper address [*ip_address*]

Syntax Definitions

ip_address DHCP server IP address (for example 21.0.0.10).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- 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.
- Using this command enables a Global DHCP Relay service on the switch. When the DHCP Relay is specified by the DHCP server IP address, the service is called Global DHCP.
- When the DHCP Relay is specified by the VLAN number of the DHCP request, the service is referred to as Per-VLAN DHCP.
- Global DHCP and Per-VLAN DHCP are mutually exclusive. You can only configure one or the other.
- Use this command to configure DHCP Relay on switches where packets are routed between IP networks.

Examples

```
-> ip helper address 75.0.0.10  
-> no ip helper address 31.0.0.20
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip helper vlan address	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 does 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 statistics	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 vlan address

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 a standard relay service is used.

ip helper vlan *vlan_id*[-*vlan_id2*] **address** *ip_address*

no ip helper vlan *vlan_id*[-*vlan_id2*] **address** *ip_address*

Syntax Definitions

<i>vlan_id</i>	VLAN identification number (for example 3) of the DHCP server VLAN.
<i>vlan_id2</i>	The last VLAN ID number in a contiguous range of VLAN IDs.
<i>ip_address</i>	IP address (for example 21.0.0.10) of the DHCP server VLAN.

Defaults

If no VLAN identification number is entered, VLAN ID 0 is used by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- 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 of VLAN ID entries. (for example, 10-15).
- The **ip helper vlan address** command works only if the **per-vlan-only** forwarding option is 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 IP interface must be defined for the VLANs before using this command.
- Use the **no** form of this command to delete the DHCP server VLAN from the DHCP Relay.

Examples

```
-> ip helper vlan 3 address 75.0.0.10
-> ip helper vlan 250-255 address 198.206.15.2
-> no ip helper vlan 3 address 75.0.0.1
-> no ip helper vlan 1601 address 198.206.15.20
```

Release History

Release 7.1.1; command 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 statistics](#)

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 the 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 10K, 6900

Usage Guidelines

To process DHCP packets on a per VLAN basis, or to change the DHCP Relay forwarding option from standard to per VLAN, use the [ip helper per-vlan-only](#) command.

Examples

```
-> ip helper standard
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show ip helper](#)

Displays current DHCP Relay configuration information.

[show ip helper statistics](#)

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 10K, 6900

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.
- To process DHCP packets on a per VLAN basis, or to change the DHCP Relay forwarding option from standard to per VLAN, use the **ip helper per-vlan-only** command.
- Using the **per-vlan-only** forwarding option requires you to specify a DHCP server IP address for each VLAN that provides a relay service. The **ip helper vlan address** command performs this function and at the same time enables relay for the specified VLAN.

Examples

```
-> ip helper per-vlan-only
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip helper vlan address	Configures a DHCP Relay service for the specified VLAN.
ip helper standard	Sets DHCP Relay forwarding option to standard. All DHCP packets are processed.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper statistics	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 sent from the client contains the elapsed boot time. This is the amount of time, in seconds, since the client last booted. DHCP Relay does not process the packet unless the elapsed boot time value of the client 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.

Defaults

By default, the forward delay time is set to three seconds.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

ip helper address	Adds or deletes one or more DHCP server IP addresses to the DHCP Relay configuration.
ip helper maximum-hops	Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper statistics	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.

Defaults

By default, the maximum hops value is set to four hops.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

ip helper address	Adds or deletes one or more DHCP server IP addresses to the DHCP Relay configuration.
ip helper forward-delay	Sets the forward delay time value. DHCP Relay does 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 statistics	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 10K, 6900

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 relay agent receives a DHCP packet that already contains the Option-82 field, the packet is processed 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 7.1.1; command introduced.

Related Commands

ip helper agent-information policy	Configures a policy to determine how the relay agent handles DHCP packets that already contain the Option-82 field.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper statistics	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 handles the 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 10K, 6900

Usage Guidelines

- 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 does not insert the relay agent information option into the DHCP packet and forwards 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 7.1.1; command introduced.

Related Commands

ip helper agent-information	Enables the insertion of relay agent information Option-82 into DHCP packets.
show ip helper	Displays current DHCP Relay configuration information.
show ip helper statistics	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 10K, 6900

Usage Guidelines

PXE support is disabled by default and it is 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 7.1.1; command introduced.

Related Commands

[show ip helper](#) Displays current DHCP Relay configuration information.

MIB Objects

iphelperPXESupport

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 10K, 6900

Usage Guidelines

- Use the **ip helper boot-up enable** command to specify BootP or DHCP for the request packet type.
- If an IP router port already exists for VLAN 1, a request packet is not broadcast even if automatic IP address configuration is enabled for the switch.

Examples

```
-> ip helper boot-up enable
-> ip helper boot-up disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip helper boot-up enable Specifies BootP or DHCP as the type of request packet the switch broadcasts 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 10K, 6900

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 7.1.1; command introduced.

Related Commands

[ip helper boot-up](#) Enables or disables automatic IP configuration for the switch.

MIB Objects

```
iphelperStatTable  
iphelperBootupPacketOption
```

ip udp relay port

Enables or disables UDP port relay for user-defined service ports that are not well-known.

ip udp relay port *port_num* [**description** *description*]

ip udp relay no port *port_num*

Syntax Definitions

port_num A service port number that is not well-known or user-defined.
description A description of the user-defined service for the specified port.

Defaults

By default, relay is enabled on the BOOTP/DHCP well-known ports.

parameter	default
<i>name</i>	UDP port #

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable the user-defined service for the specified port.
- Use the **port** parameter to specify service port numbers that are not well known.

Examples

```
-> ip udp relay port 54
-> ip udp relay port 54 description "Generic Service"
-> ip udp relay no port 54
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip udp relay service 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 service

Enables or disables UDP port relay for generic UDP service ports (NBNS, NBDD, or other well-known UDP ports).

```
ip udp relay service {TFTP | TACACS | NTP | NBNS | NBDD | DNS} [description description]
```

```
ip udp relay no service {TFTP | TACACS | NTP | NBNS | NBDD | DNS}
```

Syntax Definitions

TFTP	TFTP well-known port 69.
TACACS	TACACS well-known port 65.
NTP	NTP well-known port 123.
NBNS	NBNS well-known ports 137.
NBDD	NBDD well-known port 138.
DNS	DNS well-known port 53.
<i>description</i>	A description of the UDP service.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable UDP Relay for the specified service port.
- The *description* parameter is only used with any of the **service** keywords and provides a user-defined description to identify the port service.
- When UDP Relay is disabled for BOOTP/DHCP, the **ip helper** configuration is *not* retained and all dependant functionality (automatic IP configuration for VLAN 1, Telnet and HTTP client authentication, and so on) is disrupted.
- Up to three types of UDP Relay services are supported at any one time and in any combination.
- If port relay is enabled for the NBDD well-known port, NBNS is not automatically enabled by default.
- 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 service DNS
-> ip udp relay service DNS description DNS_1
-> ip udp relay no service DNS
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip udp relay service 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 service vlan

Specifies a VLAN on which traffic destined for a UDP port is forwarded.

ip udp relay service {TFTP | TACACS | NTP | NBNS | NBDD | DNS} | **port** *port_num* [**description** *description*] **vlan** *vlan_id*[-*vlan_id2*]

ip udp relay service {TFTP | TACACS | NTP | NBNS | NBDD | DNS} | **port** *port_num* **no vlan** *vlan_id*[-*vlan_id2*]

Syntax Definitions

TFTP	TFTP well-known port 69.
TACACS	TACACS well-known port 65.
NTP	NTP well-known port 123.
NBNS	NBNS well-known ports 137.
NBDD	NBDD well-known port 138.
DNS	DNS well-known port 53.
<i>port_num</i>	A user-defined port number.
<i>description</i>	A description of the UDP service.
<i>vlan_id</i>	A numeric value that uniquely identifies an individual VLAN.
<i>-vlan_id2</i>	The last VLAN ID number in a contiguous range of VLAN IDs. Use a hyphen to specify a range of VLANs (for example, 1-5).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the VLAN association with the UDP service port.
- The UDP port must be created before using this command.
- Use the **service** keyword to define a well-known UDP port. Use the **port** keyword to specify a user-defined port.
- 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 service DNS vlan 10
-> ip udp relay service DNS vlan 500-550
-> ip udp relay service DNS no vlan 10
-> ip udp relay port 3047 vlan 20
-> ip udp relay port 3047 no vlan 20
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip udp relay port	Enables or disables UDP port relay for user-defined service ports that are not well-known.
ip udp relay service	Enables or disables relay for UDP service ports.

MIB Objects

```
iphelperxPortServiceAssociationTable
  iphelperxPortServiceAssociationService
```

show ip helper

Displays the current DHCP Relay and Relay Agent Information.

show ip helper

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Displays information for all IP addresses configured.

Examples

The following example shows the show ip helper command output:

```
-> show ip helper
Ip helper :
  Forward Delay(seconds)           = 300,
  Max number of hops                = 5,
  Relay Agent Information           = Enabled,
  Relay Agent Information Policy    = Keep,
  PXE support                       = Enabled,
  Forward option                    = standard mode,
  Bootup Option                    = Disable,
  Bootup Packet Option              = DHCP
  Forwarding address list (Standard mode):
    128.100.16.1
```

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.
Relay Agent Information	Indicates the status (Enabled or Disabled) of the DHCP relay agent information option feature. Configured through the ip helper agent-information command.
Relay Agent Information Policy	The policy configured to determine how the DHCP relay agent handles the DHCP packets that already contain an Option-82 field.

output definitions

PXE support	Specifies the status (Enabled or Disabled) of the relay agent support for PXE devices. By default the PXE support is disabled. Configured through the ip helper pxe-support command.
Forward option	The current forwarding option setting: standard mode .
Bootup Option	Indicates whether or not automatic IP address configuration for default VLAN 1 is done when the switch boots up (Enabled or Disabled). Configured through the ip helper boot-up command.
Bootup Packet Option	Indicates if the Bootup Option broadcasts a DHCP or BOOTP packet to obtain an IP address for default VLAN 1. Configured through the ip helper boot-up enable command. Note that this field does not appear if the Bootup Option is disabled.
Forwarding Addresses	IP addresses for DHCP servers that 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 7.1.1; command introduced.

Related Commands**show ip helper statistics**

Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

iphelperTable

iphelperService
iphelperForwAddr
iphelperForwDelay
iphelperMaxHops

iphelperAgentInformation

iphelperAgentInformationPolicy

iphelperStatTable

iphelperBootupOption
iphelperBootupPacketOption

show ip helper statistics

Displays the number of packets DHCP Relay has received, the number of packets dropped due to forward delay and maximum hops violations. It also displays the number of packets processed since the last time these statistics were displayed. It 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 statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to clear all DHCP Relay statistics.

Examples

```
-> show ip helper statistics
```

```
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.

output definitions (continued)

Max Hops Violation	Number of packets dropped as a result of maximum hop violations. A violation occurs if a packet contains a hop count equal to or greater than the configured DHCP Relay maximum hops value.
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 7.1.1; command introduced.

Related Commands

show ip helper Displays current DHCP Relay configuration information.

MIB Objects

```
iphelperStatTable
  iphelperServerAddress
  iphelperRxFromClient
  iphelperTxToServer
  iphelperMaxHopsViolation
  iphelperForwDelayViolation
  iphelperResetAll
```

show ip udp relay

Displays the VLAN assignments to which the traffic received on the UDP service ports is forwarded. Displays the current configuration for UDP services by service name or by service port number.

show ip udp relay [service {TFTP | TACACS | NTP | NBNS | NBDD | DNS} | port *port_num*]

Syntax Definitions

TFTP	TFTP well-known port 69.
TACACS	TACACS well-known port 65.
NTP	NTP well-known port 123.
NBNS	NBNS well-known port 137.
NBDD	NBDD well-known ports 138.
DNS	DNS well-known port 53.
<i>port_num</i>	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 10K, 6900

Usage Guidelines

- Use the **show ip udp relay** command without the additional parameters to display information related to all the ports.
- Enter a service name with this command along with the **service** parameter to display information about an individual service.
- Mention a port number along with the **port** parameter, to get the UDP relay information for the specific user defined or well-known port.

Examples

```
-> show ip udp relay
```

```
Service          Port      VLANs
-----+-----+-----
DNS              53       2  4
TACACS          65       3
```

output definitions

Service	The active UDP service name.
----------------	------------------------------

output definitions (continued)

Port	The UDP service port number.
VLANs	The VLAN assigned to the UDP service port that forwards traffic destined for that port. Use the ip udp relay service vlan command to configure this value.

```
-> show ip udp relay service DNS
```

```
Service      Port(s)  Description
-----+-----+-----
  4           53       DNS
```

```
-> show ip udp relay port
```

```
Service      Port(s)  Description
-----+-----+-----
  4           54       Generic_Service
  5           66       Tservice
```

```
-> show ip udp relay port 54
```

```
Service      Port(s)  Description
-----+-----+-----
  4           54       Generic_Service
```

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 7.1.1; command introduced.

Related Commands

show ip udp relay statistics	Displays the current statistics for each UDP port relay service.
no ip helper statistics	Displays the VLAN assignments to which the traffic received on the specified UDP service port is forwarded.

MIB Objects

```
iphelperTable
  iphelperService
  iphelperVlan
iphelperxPropertiesTable
  iphelperxPropertiesName
  iphelperxPropertiesPort
  iphelperxPropertiesService
```

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 statistics [service {TFTP | TACACS | NTP | NBNS | NBDD | DNS}] [port
[port_num]]
```

Syntax Definitions

TFTP	TFTP well-known port 69.
TACACS	TACACS well-known port 65.
NTP	NTP well-known port 123.
NBNS	NBNS well-known port 137.
NBDD	NBDD well-known ports 138.
DNS	DNS well-known port 53.
<i>port_num</i>	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 10K, 6900

Usage Guidelines

- Enter a service name with the **service** parameter to display information about an individual service.
- Enter a port number with the **port** parameter to display information about an individual service.

Examples

```
-> show ip udp relay statistics
```

Service	Vlan	Pkts Sent	Pkts Recvd
145		0	0
DNS	2	10	10
	4	15	15
TACACS	3	0	0

```
-> show ip udp relay statistics service tacacs
```

Service	Vlan	Pkts Sent	Pkts Recvd
TACACS	3	0	0


```
-> show ip udp relay statistics port 1776
```

```
Service          Vlan    Pkts Sent  Pkts Recvd
-----+-----+-----+-----
A UDP Protocol   18      2          2
```

output definitions

Service	The active UDP service name.
VLAN	The VLAN assigned to the UDP service port that forwards traffic destined for that port. Use the ip udp relay service vlan command to configure this value.
Pkts Sent	The number of packets sent from this service port to the server.
Pkts Recvd	The number of packets received by this service port from a client.

Release History

Release 7.1.1; command introduced.

Related Commands

[show ip udp relay](#) Displays current configuration for UDP services by service name or by service port number.

MIB Objects

```
iphelperxStatTable
  iphelperxStatService
  iphelperxStatVlan
  iphelperxStatTxToServer
  iphelperxStatRxFromClient
```

no ip helper statistics

Resets the IP helper statistics for the specified VRF instances.

no ip helper statistics [**global-only** | **server-only** | **address** *ip_address* / **vlan** *vlan_id* {**address** *ip_address*}]

Syntax Definitions

global-only	Specifies that only the global IP helper statistics must be reset.
server-only	Specifies that only the IP helper statistics related to the server must be reset.
<i>ip_address</i>	Specifies the IP address for the flat mode instance.
<i>vlan_id</i>	Specifies the VLAN ID for the per-vlan mode instance.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command works only for VRF instances.
- To reset all the IP helper related statistics, use this command without the additional keywords.
- To reset the IP helper statistics for the flat mode instance, provide the related IP address with the **address** keyword
- To reset the IP helper statistics for the per-vlan mode instance, provide the VLAN ID with the **vlan** keyword and the related IP address with the **address** keyword.

Examples

```
-> no ip helper statistics
-> no ip helper statistics global-only
-> no ip helper statistics server-only
-> no ip helper statistics address 172.6.5.1
-> no ip helper statistics vlan 20 address 172.6.5.1
```

Release History

Release 7.1.1; command introduced.

Related Commands**show ip helper statistics**

Displays the current statistics for each UDP port relay service.

MIB Objects

```
iphelperStatsTable  
  iphelperResetAllStats  
  iphelperResetSrvStats
```

ip udp relay no statistics

Resets all the generic UDP Relay Service related statistics.

ip udp relay no statistics

Syntax Definitions

N/A

Defaults

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- On applying this command, the UDP relay statistics are cleared and the **show ip udp relay statistics** command display no information.

Examples

```
-> ip udp relay no statistics
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show ip udp relay statistics](#) Displays the current statistics for each UDP port relay service.

MIB Objects

```
genericUdpRelayTable  
genericUdpRelayStatReset
```

19 VRRP Commands

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure in a default route environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP/VRRP3 routers on the LAN. The VRRP/VRRP3 router, which controls the IP/IPv6 address associated with a virtual router is called the master router, and forwards packets to that IP/IPv6 address. If the master router becomes unavailable, the highest priority backup router will transition to the master state. The Alcatel-Lucent implementation of VRRP also supports the collective management of virtual routers on a switch.

Note. VRRP3 does not support the collective management functionality in this release.

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

A summary of the available VRRP commands is 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* **admin-state** [**enable** | **disable**] [**priority** *priority*] [**preempt** | **no preempt**] [[**advertising**] **interval** *seconds*]

no vrrp *vrid* *vlan_id*

Syntax Definitions

<i>vrid</i>	The virtual router ID, in the range from 1–255.
<i>vlan_id</i>	The VLAN on which the virtual router is configured. The VLAN must already be created and available on the switch.
enable	Enables the virtual router. A virtual router may only be enabled if an IP address is configured for the virtual router.
disable	Disables the virtual router. Cannot be combined on the same line with other parameters.
<i>priority</i>	The priority for this virtual router to become the master router. The range is 1 (lowest priority) to 255 (highest priority). The priority should be set to 255 only if this router is the actual owner of the virtual router's IP address.
preempt	Specifies that a higher priority router may preempt a lower priority master router.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router.
<i>seconds</i>	The interval in seconds after which the master router will send VRRP advertisements. The advertising interval must be same for all VRRP routers configured with the same VRID. The valid range is 1–255 seconds.

Defaults

parameter	default
enable disable	disable
<i>priority</i>	100
preempt no preempt	preempt
<i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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**. Note that **disable** cannot be used with any other optional parameter.
- A virtual router must be disabled before it can be modified.
- **Advertising** is an optional command parameter. When prefaced before **interval**, it displays the same information as **vrrp vrid vlan_id interval** information about configuring priority:
- A value of 255 indicates that the VRRP router owns the IP address; that is, the router contains the real physical interface to which the IP address is assigned. The system automatically sets this value to 255 if it detects that this router is the IP address owner. If the priority is set to 255 and the virtual router is not the IP address owner, then the priority will be set to the default value of 100. The IP address owner will always be the master router if it is available.
- VRRP routers backing up a virtual router must use priority values from 1 to 255. The default priority value for VRRP routers backing up a virtual router is 100. If you configure more than one backup, their priority values should be different. The **preempt** or **no preempt** setting specifies whether or not a higher priority router may preempt a lower priority master router.

Examples

```
-> vrrp 23 1 priority 75
-> vrrp 23 1 admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[vrrp address](#)

Configures an IP address for a virtual router.

[show vrrp](#)

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrp3OperTable
  alaVrrp3OperAdminState
  alaVrrp3OperPriority
  alaVrrp3OperPreemptMode
  alaVrrp3OperAdvertisementInterval
  alaVrrp3OperRowStatus
```

vrrp address

Configures an IP address for a virtual router.

```
vrrp vrid vlan_id address ipv4Addr
```

```
vrrp vrid vlan_id no address ipv4Addr
```

Syntax Definitions

<i>vrid</i>	The virtual router ID, in the range from 1–255.
<i>vlan_id</i>	The VLAN on which the virtual router is configured.
<i>ipv4Addr</i>	The virtual IP address associated with the specified virtual router.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A virtual router IP address must be configured before the virtual router can be enabled.
- **IP** is an optional command parameter. It displays the same information as **vrrp address**.

Examples

```
-> vrrp 1 3 address 10.10.3.2  
-> vrrp 1 3 no address 10.10.3.2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.
show vrrp statistics	Displays statistics about VRRP packets for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
alaVrrp3AssoIpAddrTable  
  alaVrrp3AssoIpAddrRowStatus
```

vrrp track

Creates a new tracking policy or modifies an existing tracking policy.

vrrp track *track_id* **admin-state** [**enable** | **disable**] [**priority** *value*] [**ipv4-interface** *name* / **ipv6-interface** *name* | **port** *slot/port* | **address** *address*]

no vrrp track *track_id*

Syntax Definitions

<i>track_id</i>	The ID of the tracking policy; the range is 1 to 255.
enable	Enables the tracking policy.
disable	Disables the tracking policy.
<i>value</i>	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.
<i>name</i>	The name of the IPv4 or IPv6 interface that this policy will track.
<i>slot/port</i>	The slot/port number that this policy will track.
<i>address</i>	The remote IP or IPv6 address that this policy will track.

Defaults

parameter	default
enable disable	enable
<i>value</i>	25

Platforms Supported

OmniSwitch 10K, 6900

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 admin-state enable priority 50 ipv4-interface Marketing
-> vrrp track 3 admin-state enable priority 60 ipv6-interface Sales
-> vrrp track 3 admin-state disable
```

Release History

Release 7.1.1; command was 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

<i>vrid</i>	The virtual router ID, in the range from 1–255.
<i>vlan_id</i>	The VLAN ID of the virtual router.
<i>track_id</i>	The ID of the tracking policy associated with the virtual router; the range is 1 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp track-association	Displays the tracking policies associated with virtual routers.

MIB Objects

```
alaVrrpAssoTrackTable  
  alaVrrpAssoTrackId  
  alaVrrpTrackRowStatus
```

vrrp trap

Enables or disables SNMP traps for VRRP.

vrrp trap

no vrrp trap

Syntax Definitions

N/A

Defaults

By default, SNMP traps for VRRP are enabled.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[snmp-trap filter-ip](#) Enables or disables SNMP trap filtering.

MIB Objects

```
vrrpOperGroup  
vrrpNotificationCntl
```

vrrp delay

Configures the amount of time allowed for routing tables to stabilize before virtual routers are started.

vrrp delay *seconds*

Syntax Definitions

seconds

The amount of time after a reboot that virtual routers will wait before they go active; the range is 0 to 180 seconds.

Defaults

parameter	default
<i>seconds</i>	45 seconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use this command to prevent loss of workstation connectivity before a virtual router becomes master.

Examples

```
-> vrrp delay 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[vrrp](#)

Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.

[show vrrp](#)

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

alaVRRPStartDelay

vrrp interval

Modifies the default advertising interval value assigned to the virtual routers on the switch.

vrrp interval *seconds*

Syntax Definitions

seconds The default advertising interval for the virtual routers. The valid range is 1–255 seconds.

Defaults

parameter	default
<i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Modifying the default advertising interval value will affect the value assigned by default to any new virtual routers that are created.
- To apply the new default value to the existing virtual routers, you must first disable the virtual routers, then apply the new default value using **vrrp set** command and enable the virtual routers again.
- If any of the virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual routers, then override the configured value using the **vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> vrrp interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp all

Changes the administrative status of all the virtual routers on the switch.

vrrp set

Sets the new default parameter values to existing virtual routers on the switch.

show vrrp

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

alaVrrpv2Config

 alaVrrpDefaultInterval

vrrp priority

Modifies the default priority value assigned to the virtual routers on the switch.

vrrp priority *priority*

Syntax Definitions

priority The default priority value for the virtual routers. The valid range is 1–255.

Defaults

parameter	default
<i>priority</i>	100

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Modifying the default priority value will affect the value assigned by default to any new virtual routers that are created.
- To apply the new default value to the existing virtual routers, you must first disable the virtual routers, then apply the new default value using the **vrrp set** command and enable the virtual routers again.
- If any of the virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual routers, then override the configured value using the **vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> vrrp priority 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp all	Changes the administrative status of all the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrpv2Config  
  alaVrrpDefaultPriority
```

vrrp preempt

Modifies the default preempt mode assigned to the virtual routers on the switch.

vrrp [preempt | no preempt]

Syntax Definitions

preempt	Specifies that a higher priority router may preempt a lower priority master router by default.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router by default.

Defaults

parameter	default
preempt no preempt	preempt

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Modifying the default preempt mode will affect the mode assigned by default to any new virtual routers that are created.
- To apply the new default value to the existing virtual routers, you must first disable the virtual routers, then apply the new default value using the **vrrp set** command and enable the virtual routers again.
- If any of the virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual routers, then override the configured value using the **vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> vrrp preempt
-> vrrp no preempt
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp all

Changes the administrative status of all the virtual routers on the switch.

vrrp set

Sets the new default parameter values to existing virtual routers on the switch.

show vrrp

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

alaVrrpv2Config

alaVrrpDefaultPreemptMode

vrrp all

Changes the administrative status of all the virtual routers on the switch.

vrrp admin-state [**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 10K, 6900

Usage Guidelines

- This command changes the administrative status of all the virtual routers on the switch by executing a single command.
- This command will not affect the ability to change the administrative status of an individual virtual router.

Examples

```
-> vrrp admin-state disable
-> vrrp admin-state enable
-> vrrp admin-state enable-all
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp interval	Modifies the default advertising interval value assigned to the virtual routers on the switch.
vrrp priority	Modifies the default priority value assigned to the virtual routers on the switch.
vrrp preempt	Modifies the default preempt mode assigned to the virtual routers on the switch.
vrrp set	Sets the new default parameter values to existing virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

alaVrrpv2Config
alaVrrpAdminState

vrrp set

Sets the new default parameter values to existing virtual routers on the switch.

```
vrrp set [interval | priority | preempt | all | none] [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.
none	Resets all the parameter values to their default values.
override	Overrides the specified parameters configured value with the new default value.

Defaults

parameter	default
interval priority preempt all	all

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- All the virtual routers must be disabled before using this command.
- To apply the new default value to the existing virtual routers, you must first disable the virtual routers, then apply the new default value using the **vrrp set** command and enable the virtual routers again.
- If any of the virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual routers, then override the configured value using the **vrrp set** command with the **override** option and enable the virtual routers again.

Examples

```
-> vrrp set priority
-> vrrp set priority override
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp interval	Modifies the default advertising interval value assigned to the virtual routers on the switch.
vrrp priority	Modifies the default priority value assigned to the virtual routers on the switch.
vrrp preempt	Modifies the default preempt mode assigned to the virtual routers on the switch.
vrrp all	Changes the administrative status of all the virtual routers on the switch.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrpv2Config  
  alaVrrpSetParam  
  alaVrrpOverride
```

vrrp group

Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.

vrrp group *vrgid* [*interval seconds*] [*priority priority*] [**preempt** | **no preempt**]

no vrrp group *vrgid*

Syntax Definitions

<i>vrgid</i>	The virtual router group ID, in the range from 1–255.
<i>seconds</i>	The default advertising interval for the virtual router group. The valid range is 1–255 seconds.
<i>priority</i>	The default priority value for the virtual router group. The valid range is 1–255.
preempt	Specifies that a higher priority router may preempt a lower priority master router by default.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router by default.

Defaults

parameter	default
<i>seconds</i>	1
<i>priority</i>	100
preempt no preempt	preempt

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the virtual router group.
- The configuration parameters can be modified at any time, but will not have any effect on the virtual routers in the group until the virtual routers are enabled again. To apply the group default value to the virtual routers in a group, you must first disable the virtual router group, then apply the group default value using the **vrrp group set** command and enable the virtual router group again.
- If any of the virtual routers in the group are running with their configured value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual router group, then override the configured value by using the **vrrp group set** command with the **override** option and enable the virtual router group again.
- When a virtual router group is deleted, the virtual routers assigned to the group become unassigned. However, this does not have any impact on the virtual routers.

Examples

```
-> vrrp group 25 interval 50 priority 50 no preempt
-> no vrrp group 25
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp group all	Changes the administrative status of all the virtual routers in a virtual router group using a single command.
vrrp group set	Sets the new modified default value to all the virtual routers in a virtual router group.
vrrp group-association	Adds a virtual router to a virtual router group.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

```
alaVrrpGroupTable
  alaVrrpGroupInterval
  alaVrrpGroupPriority
  alaVrrpGroupPreemptMode
  alaVrrpGroupRowStatus
```

vrrp group all

Changes the administrative status of all the virtual routers in a virtual router group using a single command.

vrrp group *vrgid* admin-state [disable | enable | enable-all]

Syntax Definitions

<i>vrgid</i>	The virtual router group ID, in the range from 1–255.
disable	Disables all the virtual routers in the group.
enable	Enables those virtual routers that have not previously been disabled individually in the group.
enable-all	Enables all the virtual routers in the group including those virtual routers that have been disabled individually.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If a virtual router in a group is disabled on an individual basis, it can only be reenabled by using the **enable-all** option in this command.
- This command will not affect the ability to change the administrative status of an individual virtual router.

Examples

```
-> vrrp group 25 admin-state disable  
-> vrrp group 25 admin-state enable  
-> vrrp group 25 admin-state enable-all
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp group	Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
vrrp group set	Sets the new modified default value to all the virtual routers in a virtual router group.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

alaVrrpGroupTable
 alaVrrpGroupAdminState

vrrp group set

Sets the new modified default value to all the virtual routers in a virtual router group.

vrrp group *vrgid* set [interval | priority | preempt | all] [override]

Syntax Definitions

<i>vrgid</i>	The virtual router group ID, in the range from 1–255.
interval	Sets the VRRP advertisement interval value to the new default value.
priority	Sets the priority value to the new default value.
preempt	Sets the preempt mode to the new default mode.
all	Sets all the parameters' value to the new default value.
override	Overrides the parameter's configured value with the group default value.

Defaults

parameter	default
interval priority preempt all	all

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- All the virtual routers must be disabled before using this command.
- To apply the group default value to the virtual routers in a group, you must disable the virtual router group, then apply the group default value using the **vrrp group set** command and enable the virtual router group again.
- If any of the virtual routers in the group are running with their own configured parameter value, then that value will take priority over the group default value. To override the configured value with the group default value, you must first disable the virtual router group, then override the configured value by using the **vrrp group set** command with the **override** option and enable the virtual router group again.

Examples

```
->vrrp group 10 set priority
->vrrp group 10 set priority override
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp group	Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
vrrp group all	Changes the administrative status of all the virtual routers in a virtual router group using a single command.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.
show vrrp group	Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

```
alaVrrpGroupTable  
  alaVrrpGroupSetParam  
  alaVrrpGroupOverride
```

vrrp group-association

Adds a virtual router to a virtual router group.

```
vrrp vrid vlan_id group-association vrgid
```

```
vrrp vrid vlan_id no group-association vrgid
```

Syntax Definitions

<i>vrid</i>	The virtual router ID, in the range from 1–255.
<i>vlan_id</i>	The VLAN on which the virtual router is configured. The VLAN must already be created and available on the switch.
<i>vrgid</i>	The virtual router group ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the virtual router from the virtual router group.
- A virtual router need not be disabled in order to be added to a virtual router group. However, the virtual router will not adopt the group's default parameter values until it is reenabled.
- A virtual router need not be disabled to be removed from a group.

Examples

```
-> vrrp 25 1 group-association 10  
-> vrrp 25 1 no group-association 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show vrrp group-association](#) Displays the virtual routers that are associated with a group.

MIB Objects`alaVrrpAssoGroupTable``alaVrrpAssoGroupRowStatus`

vrrp3

Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.

vrrp3 *vrid* *vlan_id* **admin-state** [**enable** | **disable**] [**priority** *priority*] [**preempt** | **no preempt**][**accept** | **no accept**] [[**advertising**] **interval** *centiseconds*]

no vrrp3 *vrid* *vlan_id*

Syntax Definitions

<i>vrid</i>	The virtual router ID, in the range from 1–255.
<i>vlan_id</i>	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.
<i>priority</i>	The priority for this virtual router to become the master router. The range is 1 (lowest priority) to 255 (highest priority). The priority should be set to 255 only if this router is the actual owner of the virtual router's IP address.
preempt	Specifies that a higher priority router may preempt a lower priority master router.
no preempt	Specifies that a higher priority router may not preempt a lower priority master router.
accept	Specifies that the master router, which is not the IPv6 address owner will accept the packets addressed to the IPv6 address owner as its own.
no accept	Specifies that the master router, which is not the IPv6 address owner will not accept the packets addressed to the IPv6 address owner as its own.
<i>centiseconds</i>	The interval in centiseconds after which the master router will send VRRP3 advertisements. The advertising interval must be the same for all VRRP3 routers configured with the same VRID. The valid range is 1–4096 centiseconds.

Defaults

parameter	default
enable disable	disable
<i>priority</i>	100
preempt no preempt	preempt
accept / no accept	accept
<i>centiseconds</i>	100

Platforms Supported

OmniSwitch 10K, 6900

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** option. Note that the **disable** option cannot be used with any other optional parameter.
- A virtual router must be disabled before it can be modified.
- The maximum number of virtual routers supported is based on the 100 centisecond interval. A smaller interval will result in a relatively lesser number of virtual routers.
- The advertising interval cannot be less than 10 centiseconds.
- **Advertising** is an optional command parameter. When prefaced before **interval**, it displays the same information as **vrrp3 vrid vlan_id interval**.

Examples

```
-> vrrp3 23 1 priority 75
-> vrrp3 23 1 admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[vrrp3 address](#)

Configures an IPv6 address for a virtual router.

[show vrrp3](#)

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```
alaVrrp3OperTable  
  alaVrrp3OperAdminState  
  alaVrrp3OperPriority  
  alaVrrp3OperPreemptMode  
  alaVrrp3OperAcceptMode  
  alaVrrp3OperAdvinterval  
  alaVrrp3OperRowStatus
```

vrrp3 address

Configures an IPv6 address for a virtual router.

```
vrrp3 vrid vlan_id address [ipv6Addr | ipv6v4Addr]
```

```
vrrp3 vrid vlan_id no address [ipv6Addr | ipv6v4Addr]
```

Syntax Definitions

<i>vrid</i>	The virtual router ID, in the range from 1–255.
<i>vlan_id</i>	The VLAN on which the virtual router is configured.
<i>address</i>	The virtual IPv6 address associated with the specified virtual router.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

IP is an optional command parameter. It displays the same information as **vrrp3 address**.

Examples

```
-> vrrp3 1 3 address 213:100:1::56  
-> vrrp3 1 3 no address 213:100:1::56
```

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp3	Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp3 statistics	Displays statistics for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
alaVrrp3AssoIpAddrTable  
  alaVrrp3AssoIpAddrRowStatus
```

vrrp3 trap

Enables or disables SNMP traps for VRRP3.

vrrp3 trap

no vrrp3 trap

Syntax Definitions

N/A

Defaults

By default, SNMP traps for VRRP3 are enabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

SNMP traps must be enabled globally on the switch for VRRP3 traps to actually be sent.

Examples

```
-> vrrp3 trap  
-> no vrrp3 trap
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[snmp-trap filter-ip](#) 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

<i>vrid</i>	The virtual router ID, in the range from 1–255.
<i>vlan_id</i>	The VLAN ID of the virtual router.
<i>track_id</i>	The ID of the tracking policy associated with the virtual router; the range is 1 to 255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

vrrp3	Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp3 track-association	Displays the tracking policies associated with VRRP3 virtual routers.

MIB Objects

```
alaVrrp3AssoTrackTable  
  alaVrrp3AssoTrackId  
  alaVrrp3TrackRowStatus
```

show vrrp

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

show vrrp [*vrid*]

Syntax Definitions

vrid The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **show vrrp** command to display information about configuration parameters, which may be set through the **vrrp** command. Use the **show vrrp statistics** command to get information about VRRP packets.

Examples

The following is an example of the output display on an OmniSwitch 10K, 6900:

```
-> show vrrp
VRRP trap generation: Enabled
VRRP startup delay: 75

  VRID  VLAN      IP Address(es)  Admin Status  Priority  Preempt  Adv. Interval
-----+-----+-----+-----+-----+-----+-----+
    1    1     192.168.170.1  Enabled  255     Yes      1
      192.168.170.2
    2   15     10.2.25.254   Disabled 100     No       1
```

The following is an example of the output display on an OmniSwitch 10K, 6900:

```
-> show vrrp
VRRP default advertisement interval: 5 seconds
VRRP default priority: 100
VRRP default preempt: Yes
VRRP trap generation: Enabled
VRRP startup delay: 45 (expired)

  VRID  VLAN      IP Address(es)  Admin Status  Priority  Preempt  Adv. Interval
-----+-----+-----+-----+-----+-----+-----+
    1   101  192.60.245.240  Enabled  100  Yes      5
    2   102  192.60.246.240  Enabled  100  Yes      5
```

```

-> show vrrp 1
Virtual Router VRID = 1 on VLAN = 1
  Admin Status      = Enabled
  Priority          = 255
  Preempt          = Yes
  Adv. Interval    = 1
  Virtual MAC      = 00-00-5E-00-02-01
  IP Address(es)
    192.168.170.1
    192.168.170.2

```

output definitions

VRRP default advertisement interval	The default advertising interval for all virtual routers on the switch.
VRRP default priority	The default priority value for all virtual routers on the switch.
VRRP default preempt	The default preempt mode for all virtual routers on the switch.
VRRP trap generation	Indicates whether or not the VRRP trap generation is enabled or disabled; configured through the vrrp track command.
VRRP startup delay	The amount of time after a reboot that virtual routers will wait before they go active; allows time for routing tables to stabilize. Configured through the vrrp delay command.
VRID	Virtual router identifier. Configured through the vrrp command.
VLAN	The VLAN associated with the VRRP instance. Configured through the vrrp command.
IP Address(es)	The assigned IP addresses. Configured through the vrrp address command.
Admin Status	The administrative status of this virtual router instance; enabled allows the virtual router instance to operate; disabled disables the virtual router instance without deleting it.
Priority	Indicates the VRRP router's priority for the virtual router. For more information about priority, see the vrrp command description on page 19-3 .
Preempt	Controls whether a higher priority virtual router will preempt a lower priority master router: preempt indicates that a higher priority virtual router will preempt a lower priority master; no preempt indicates that the first backup router to take over for the master will not be preempted by a virtual router with a higher priority. In either case, the IP address owner will always take over it if is available.
Virtual MAC	Displays the virtual MAC address for the virtual router. The first 5 bytes are always 00-00-5E-00-02. The last byte indicates the VRID. This field displays N/A when the virtual router is in the backup or initialize state.
Adv. Interval	Indicates the time interval, in seconds, between sending advertisement messages. Only the master router sends advertisements.

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.
vrrp address	Configures an IP address for a virtual router.
vrrp interval	Modifies the default advertising interval value assigned to the virtual routers on the switch.
vrrp priority	Modifies the default priority value assigned to the virtual routers on the switch.
vrrp preempt	Modifies the default preempt mode assigned to the virtual routers on the switch.
show vrrp statistics	Displays statistics for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
alaDispVrpp3Config  
  alaVRRPDefaultInterval  
  alaVRRPDefaultPriority  
  alaVRRPDefaultPreemptMode  
  alaVrrp3AssoIpAddr  
  alaVrrp3OperAdminState  
  alaVrrp3OperPriority  
  alaVrrp3OperPreemptMode  
  alaVrrp3OperAcceptMode
```

show vrrp statistics

Displays statistics about VRRP packets for all virtual routers configured on the switch or for a specific virtual router.

show vrrp [*vrid*] **statistics**

Syntax Definitions

vrid The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **show vrrp statistics** command to display information about VRRP packets. Use the **show vrrp** command to display information about the virtual router configuration.

Examples

```
-> show vrrp statistics
```

```
Checksum   Version   VRID
Errors     Errors   Errors
-----+-----+-----
           0         0         0

VRID  VLAN  State           UpTime  Become Master  Adv. Rcvd
-----+-----+-----+-----+-----+-----
  1    1  master          378890          1           0
  2   15 backup            4483           0          44
  7    2 initialize           0           0           0
```

output definitions

Checksum Errors	The total number of VRRP packets received with an invalid checksum value.
Version Errors	The total number of VRRP packets received with an invalid version number.
VRID Errors	The total number of VRRP packets received with invalid VRIDs.
VRID	The virtual router identifier.
VLAN	The VLAN associated with the VRRP instance.

output definitions (continued)

State	The operational state of the VRRP router instance; initialize specifies that the interface or VLAN is either disabled or down, or if the startup delay timer has not expired; backup specifies that this instance is monitoring the availability of the master router; master specifies that this instance is functioning as the master router.
UpTime	Time interval (in hundredths of a second) since this virtual router was last initialized.
Become Master	The total number of times this virtual router's state has transitioned from backup to master.
Adv. Rcvd	The total number of VRRP advertisements received by this instance.

```
-> show vrrp 1 statistics
Virtual Router VRID = 1 on VLAN = 1
  State = master
  UpTime (1/100th second) = 378890
  Become master = 1
  Advertisements received = 0
  Type errors = 0
  Advertisement interval errors = 0
  Authentication errors = 0
  IP TTL errors = 0
  IP address list errors = 0
  Packet length errors = 0
  Zero priority advertisements sent = 0
  Zero priority advertisements received = 0
```

output definitions

VRID	The virtual router identifier.
VLAN	The VLAN associated with the VRRP instance.
State	The operational state of this VRRP router instance; initialize specifies that the interface or VLAN is either disabled or down, or the startup delay timer has not expired; backup specifies that this instance is monitoring the availability of the master router; master specifies that this instance is functioning as the master router.
UpTime	Time interval (in hundredths of a second) since this virtual router was last initialized.
Become master	The total number of times this virtual router's state has transitioned from backup to master.
Advertisements received	The total number of VRRP advertisements received by this instance.
Type errors	The total number of VRRP packets received with an invalid value in the VRRP type field.
Advertisement interval errors	The total number of VRRP packets received in which the advertisement interval differs from the one configured for the virtual router.
Authentication errors	The total number of VRRP packets received with an unknown or invalid authentication type.
IP TTL errors	The total number of VRRP packets received with a TTL value other than 255.

output definitions (continued)

IP address list errors	The total number of VRRP packets in which the IP address list does not match the configured list for the virtual router.
Packet length errors	The total number of VRRP packets received with a length less than the length of the VRRP header.
Zero priority advertisements sent	The total number of VRRP advertisements with a priority of 0 sent by the virtual router.
Zero priority advertisements received	The total number of VRRP advertisements with a priority of 0 received by the virtual router.

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp	Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.
show vrrp	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```

alaVrrp3RouterChecksumErrors
alaVrrp3RouterVersionErrors
alaVrrp3RouterVrIdErrors
alaVrrp3RouterStatsTable
  alaVrrp3StatsBecomeMaster
  alaVrrp3StatsAdvertiseRcvd
  alaVrrp3StatsAdvIntervalErrors
  alaVrrp3StatsIpTtlErrors
  alaVrrp3StatsPriZeroPktsRcvd
  alaVrrp3StatsPriZeroPktsSent
  alaVrrp3StatsInvalidTypePktsRcvd
  alaVrrp3StatsAddressListErrors
  alaVrrp3StatsInvlAuthType
  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 10K, 6900

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
ID          Policy          Admin   Oper
           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 7.1.1; command was introduced.

Related Commands

vrrp track

Creates a new tracking policy or modifies an existing tracking policy.

MIB Objects

```
alaVRRPTrackTable  
  alaVrrpTrackState  
  alaVrrpTrackAdminState  
  alaVrrpTrackPriority  
  alaVrrpTrackEntityType  
  alaVrrpTrackEntityVlan  
  alaVrrpTrackEntityPort  
  alaVrrpTrackEntityIpAddress  
  alaVrrpTrackEntityIpv6Interface  
  alaVrrpTrackEntityInterface
```

show vrrp track-association

Displays the tracking policies associated with virtual routers.

show vrrp [*vrid*] **track-association** [*track_id*]

Syntax Definitions

<i>vrid</i>	The virtual router ID, in the range from 1–255.
<i>track_id</i>	The ID of the tracking policy for which you want to display information.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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
```

VRID	VLAN	Conf Pri	Cur Pri	Track ID	Policy	Admin State	Oper State	Track Pri
2	1	100	100	1	VLAN 1	Enabled	Up	25
				2	10.255.11.101	Enabled	Up	25

output definitions

VRID	The virtual router identifier.
VLAN	The VLAN ID associated with the virtual router.
Conf Pri	The priority configured for the virtual router through the vrrp command.
Cur Pri	The priority currently being used for the virtual router. If the tracking policy is in effect because the tracked entity is down, the current priority will be equal to the configured priority (Conf Pri) minus the tracking priority (Track Pri). Otherwise the current priority will be equal to the configured priority.
Track ID	The ID of the tracking policy.
Policy	The VLAN, IP address, or slot/port being tracked by this policy.

output definitions (continued)

Admin State	The administrative state of the tracking policy configured through the vrrp track command.
Oper State	Whether the tracking policy is operational (Up) or not (Down).
Track Pri	The amount to be decremented from the configured virtual router priority when the tracking policy is applied.

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp track-association	Associates a VRRP tracking policy with a virtual router.
vrrp track	Creates a new tracking policy or modifies an existing tracking policy.

MIB Objects

```

alaVrrpAssoTrackTable
  alaVrrpAssoTrackId
alaVRRPTrackTable
  alaVrrpTrackState
  alaVrrpTrackAdminState
  alaVrrpTrackPriority
  alaVrrpTrackEntityType
  alaVrrpTrackEntityVlan
  alaVrrpTrackEntityPort
  alaVrrpTrackEntityIpAddress
  alaVrrpTrackEntityInterface

```

show vrrp group

Displays the default parameter values for all the virtual router groups or for a specific virtual router group.

`show vrrp group [vrgid]`

Syntax Definitions

vrgid The virtual router group ID, in the range from 1–255.

Defaults

By default, the default parameter values are displayed for all the virtual router groups.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *vrgid* parameter with this command to display the default values for a specific virtual router group.

Examples

```
-> show vrrp group 2
Virtual Router Group GROUPID = 2
  Interval = 11
  Priority = 250
  Preempt Mode = Yes
  3 Associated Virtual Routers
```

output definitions

Group ID	The virtual router group identifier.
Adv Interval	Indicates the time interval, in seconds, between the sending of advertisement messages. Only the master router sends advertisements.
Priority	Indicates the VRRP router's priority for the virtual router group. For more information about priority, see the vrrp command description on page 19-3 .
Preempt Mode	Controls whether a higher priority virtual router will preempt a lower priority master; preempt indicates that a higher priority virtual router will preempt a lower priority master; no preempt indicates that the first backup router to take over for the master will not be preempted by a virtual router with a higher priority. In either case, the IP address owner will always take over it if is available.

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp group

Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.

vrrp group all

Changes the administrative status of all the virtual routers in a virtual router group using a single command.

MIB Objects

alaVrrpGroupTable
 alaVrrpGroupInterval
 alaVrrpGroupPriority
 alaVrrpGroupPreemptMode

show vrrp group-association

Displays the virtual routers that are associated with a group.

show vrrp group-association [*vrgid*]

Syntax Definitions

vrgid The virtual router group ID, in the range from 1–255.

Defaults

By default, all virtual router group associations are displayed.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands**vrrp group-association**

Adds a virtual router to a virtual router group.

MIB Objects

alaVrrpAssoGroupTable

 alaVrrp3OperVrId

show vrrp3

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

```
show vrrp3 [vrid]
```

Syntax Definitions

vrid The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **show vrrp3** command to display information about configuration parameters, which may be set through the **vrrp3** command. Use the **show vrrp3 statistics** command to get information about VRRP3 packets.

Examples

```
-> show vrrp3
VRRP trap generation: Enabled
VRRP startup delay: 45 (expired)
```

VRID	VLAN	IPv6 Address(es)	Admin Status	Priority	Preempt	Accept	Adv. Interval
1	101	fe80::200:5eff:fe00:201 1010::30	Enabled	200	No	Yes	100
2	102	fe80::200:5eff:fe00:202 1020::30	Enabled	200	No	Yes	100
3	103	fe80::200:5eff:fe00:203 1030::30	Enabled	200	No	Yes	100
4	104	fe80::200:5eff:fe00:204 1040::30	Enabled	200	No	Yes	100
5	105	fe80::200:5eff:fe00:205 1050::30	Enabled	200	No	Yes	100
6	106	fe80::200:5eff:fe00:206 1060::30	Enabled	200	No	Yes	100
7	107	fe80::200:5eff:fe00:207 1070::30	Enabled	200	No	Yes	100
8	108	fe80::200:5eff:fe00:208 1080::30	Enabled	200	No	Yes	100
9	109	fe80::200:5eff:fe00:209 1090::30	Enabled	200	No	Yes	100
10	110	fe80::200:5eff:fe00:20a 1100::30	Enabled	200	No	Yes	100

output definitions

VRRP trap generation	Whether or not VRRP trap generation is enabled or disabled.
VRRP startup delay	The amount of time after a reboot that virtual routers will wait before they go active; allows time for routing tables to stabilize.
VRID	Virtual router identifier. Configured through the vrrp3 command.
VLAN	The VLAN associated with the VRRP3 instance. Configured through the vrrp3 command.
IPv6 Address(es)	The assigned IPv6 addresses. Configured through the vrrp3 address command.
Admin Status	The administrative status of this virtual router instance; enabled allows the virtual router instance to operate; disabled disables the virtual router instance without deleting it.
Priority	Indicates the VRRP3 router's priority for the virtual router. For more information about priority, see the vrrp3 command description on page 19-29 .
Preempt	Controls whether a higher priority virtual router will preempt a lower priority master: preempt indicates that a higher priority virtual router will preempt a lower priority master; no preempt indicates that the first backup router to take over for the master will not be preempted by a virtual router with a higher priority. In either case the IP address owner will always take over it if is available.
Accept	Displays whether the master router, which is not the IPv6 address owner will accept the packets addressed to the IPv6 address owner as its own.
Virtual MAC	Displays the virtual MAC address for the virtual router when the router is in the master state. The first 5 bytes are always 00-00-5E-00-02. The last byte indicates the VRID. This field displays N/A when the virtual router is in the backup or initialize state.
Adv. Interval	Indicates the time interval, in seconds, between sending advertisement messages. Only the master router sends advertisements.

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp3	Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.
vrrp3 address	Configures an IPv6 address for a virtual router.
show vrrp3 statistics	Displays statistics for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

```
alaVrrp3OperTable  
  alaVrrp3OperAdminState  
  alaVrrp3OperPriority  
  alaVrrp3OperPreemptMode  
  alaVrrp3OperAcceptMode  
  alaVrrp3OperAdvinterval
```

show vrrp3 statistics

Displays statistics about VRRP3 packets for all virtual routers configured on the switch or for a specific virtual router.

show vrrp3 [*vrid*] statistics

Syntax Definitions

vrid The virtual router ID, in the range from 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **show vrrp3 statistics** command to display information about VRRP3 packets. Use the **show vrrp3** command to display information about the virtual router configuration.

Examples

```
-> show vrrp3 statistics
Checksum   Version   VRID
Errors     Errors    Errors
-----+-----+-----
              0          0          0

VRID VLAN   State      UpTime    Become Master Adv. Rcvd
-----+-----+-----+-----+-----+-----
  1  101 Master      2983           1         0
  2  102 Master    60675          1         0
  3  103 Master    60675          1         0
  4  104 Master    60675          1         0
  5  105 Master    60675          1         0
  6  106 Master    60675          1         0
  7  107 Master    60675          1         0
  8  108 Master    60675          1         0
  9  109 Master    60675          1         0
 10  110 Master    60675          1         0
```

output definitions

Checksum Errors	The total number of VRRP3 packets received with an invalid checksum value.
Version Errors	The total number of VRRP3 packets received with an invalid version number.
VRID Errors	The total number of VRRP3 packets received with invalid VRIDs.
VRID	The virtual router identifier.

output definitions (continued)

VLAN	The VLAN associated with the VRRP3 instance.
State	The administrative state of the VRRP3 instance; initialize specifies that the interface or vlan is either disabled or down and the startup delay timer has not expired; backup specifies that this instance is monitoring the availability of the master router; master specifies that this instance is functioning as the master router.
UpTime	Time interval (in hundredths of a second) since this virtual router was last initialized.
Become Master	The total number of times this virtual router's state has transitioned from backup to master.
Adv. Rcvd	The total number of VRRP3 advertisements received by this instance.

Release History

Release 7.1.1; command was introduced.

Related Commands

vrrp3	Configures a new VRRP3 virtual router or modifies an existing one. Used to enable or disable a virtual router.
show vrrp3	Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

```

alaVrrp3RouterChecksumErrors
alaVrrp3RouterVersionErrors
alaVrrp3RouterVrIdErrors
alaVrrp3RouterStatsTable
  alaVrrp3StatsBecomeMaster
  alaVrrp3StatsAdvertiseRcvd
  alaVrrp3StatsAdvIntervalErrors
  alaVrrp3StatsIpTtlErrors
  alaVrrp3StatsPriZeroPktsRcvd
  alaVrrp3StatsPriZeroPktsSent
  alaVrrp3StatsInvalidTypePktsRcvd
  alaVrrp3StatsAddressListErrors
  alaVrrp3StatsInvldAuthType
  alaVrrp3StatsPacketLengthErrors
alaVrrp3OperTable
  alaVrrp3OperUpTime
alaVrrp3OperGroup
  alaVrrp3OperState

```

show vrrp3 track-association

Displays the tracking policies associated with VRRP3 virtual routers.

show vrrp3 [*vrid*] **track-association** [*track_id*]

Syntax Definitions

vrid The virtual router ID, in the range from 1–255.

track_id The ID of the tracking policy for which you want to display information.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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
VRID VLAN Pri  Pri  ID          Policy      Admin  Oper  Track
-----+-----+-----+-----+-----+-----+-----+-----+-----+
      1  101  200  200  1  PORT 1/37      Enabled  Up    25
```

output definitions

VRID	The virtual router identifier.
VLAN	The VLAN ID associated with the virtual router.
Conf Pri	The priority configured for the virtual router through the vrrp3 command.
Cur Pri	The priority currently being used for the virtual router. If the tracking policy is in effect because the tracked entity is down, the current priority will be equal to the configured priority (Conf Pri) minus the tracking priority (Track Pri). Otherwise the current priority will be equal to the configured priority.
Track ID	The ID of the tracking policy.
Policy	The VLAN, IPv6 address, or slot/port being tracked by this policy.
Admin State	The administrative state of the tracking policy.

output definitions (continued)

Oper State	Indicates whether the tracking policy is operational (Up) or not (Down).
Track Pri	The amount to be decremented from the configured virtual router priority when the tracking policy is applied.

Release History

Release 7.1.1; command was introduced.

Related Commands

[vrrp3 track-association](#) Associates a VRRP3 tracking policy with a virtual router.

MIB Objects

alaVrrpTrackTable

- alaVrrpTrackState
- alaVrrpTrackAdminState
- alaVrrpTrackPriority
- alaVrrpTrackEntityType
- alaVrrpTrackEntityVlan
- alaVrrpTrackEntityPort
- alaVrrpTrackEntityIpAddress
- alaVrrpTrackEntityIpv6Interface
- alaVrrpTrackEntityInterface
- alaVrrpTrackRowStatus

alaVrrp3AssoTrackTable

- alaVrrp3AssoTrackId
- alaVrrp3TrackRowStatus

20 OSPF Commands

Open Shortest Path First routing (OSPF) is a shortest path first (SPF) or link-state protocol. OSPF is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPF chooses the least-cost path as the best path.

Each participating router distributes its local state (i.e., the router's usable interfaces and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. This database is built from the collected link state advertisements of all routers. Each multi-access network that has at least two attached routers has a designated router and a backup designated router. The designated router floods a link state advertisement for the multi-access network and has other special responsibilities.

OSPF allows collections of contiguous networks and hosts to be grouped together. A group, together with the routers having interfaces to any one of the included networks, is called an *area*. Each area runs a separate copy of the basic link-state routing algorithm. This means that each area has its own topological database, as explained in the previous section.

Alcatel-Lucent's version of OSPF complies with RFCs 1370, 1850, 2328, 2370, 3101, and 3623.

MIB information for OSPF is as follows:

Filename: AlcatelIND1DrcTm.mib
Module: ALCATEL-IND1-DRCTM-MIB

Filename: AlcatelIND1Ospf.mib
Module: ALCATEL-IND1-OSPF-MIB

Filename: IETF_OSPF.MIB
Module: OSPF-MIB

The following is a list of the commands for configuring OSPF:

Global OSPF Commands	<pre> ip ospf admin-state ip load ospf ip ospf asbr ip ospf exit-overflow-interval ip ospf extlsdb-limit ip ospf host ip ospf mtu-checking ip ospf default-originate ip ospf default-originate ip ospf default-originate ip ospf route-tag ip ospf spf-timer ip ospf virtual-link ip ospf neighbor show ip ospf show ip ospf border-routers show ip ospf ext-lsdb show ip ospf host show ip ospf lsdb show ip ospf neighbor show ip ospf routes show ip ospf routes show ip ospf routes show ip ospf virtual-link show ip ospf virtual-neighbor </pre>
OSPF Area Commands	<pre> ip ospf area ip ospf area default-metric ip ospf area range show ip ospf area show ip ospf area range show ip ospf area stub </pre>
OSPF Interface Commands	<pre> ip ospf interface ip ospf interface admin-state ip ospf interface area ip ospf interface auth-key ip ospf interface auth-type ip ospf interface dead-interval ip ospf interface hello-interval ip ospf interface md5 ip ospf interface md5 key ip ospf interface type ip ospf interface cost ip ospf interface poll-interval ip ospf interface priority ip ospf interface retrans-interval ip ospf interface transit-delay show ip ospf interface </pre>
OSPF Graceful Restart Commands	<pre> ip ospf restart-support ip ospf restart-interval ip ospf restart-helper admin-state ip ospf restart-helper strict-lsa-checking admin-state ip ospf restart initiate show ip ospf restart </pre>

ip ospf admin-state

Enables or disables the administration status of OSPF on the router.

ip ospf admin-state {enable | disable}

Syntax Definitions

enable	Enables OSPF.
disable	Disables OSPF.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The OSPF protocol must be enabled for it to route traffic.

Examples

```
-> ip ospf admin-state enable
-> ip ospf admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf](#) Displays OSPF status and general configuration parameters.

MIB Objects

```
ospfGeneralGroup
  ospfAdminStat
```

ip load ospf

Loads the OSPF software on the router.

ip load ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Example

```
-> ip load ospf
```

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

ALADRCTMCONFIG

alaDrcTmIPOspfStatus

ip ospf asbr

Configures the router as an Autonomous System Border Router (ASBR). A router running multiple protocols or acting as a gateway to other exterior routers is an ASBR. *This command is currently not supported.*

ip ospf asbr

no ip ospf asbr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Autonomous System Border Routers (ASBRs) are routers that exchange information with routers from another autonomous system (AS).
- The **no** variant of this command removes the ASBR classification of the selected router.

Examples

```
-> ip ospf asbr
-> no ip ospf asbr
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf](#)

Displays OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
  alaOspfAsBdRtr
```

ip ospf exit-overflow-interval

This command sets the overflow interval value.

ip ospf exit-overflow-interval *seconds*

Syntax Definitions

seconds The number of seconds the router waits before attempting to leave the overflow state.

Defaults

parameter	default
<i>seconds</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The overflow interval is the time whereby the routing router will wait before attempting to leave the database overflow state; the interval begins upon the routing router's arrival into this state.
- When the routing router leaves the overflow state, it can once again create non-default and external link state advertisements (LSAs) for autonomous systems (AS).
- Note that the router will not leave the overflow state (until it is restarted) when the overflow interval value is set to 0.

Example

```
-> ip ospf exit-overflow-interval 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf](#) Displays the OSPF status and general configuration parameters.

MIB Objects

ospfGeneralGroup
 ospfExitOverflowInterval

ip ospf extlsdb-limit

Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.

ip ospf extlsdb-limit *limit*

Syntax Definitions

limit

The maximum number of LSDB entries allowed on the router. The accepted value is any number greater than or equal to 1. If 0 is entered, there is no limit.

Defaults

parameter	default
<i>limit</i>	-1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows you to set a limit to the number of external LSDBs learned by the router. An external LSDB is created when the router learns a link address that exists outside of its Autonomous System (AS).
- When the limit is set, and it is exceeded, older addresses that were previously learned are removed from the routing table to make room for the new external LSDB.

Example

```
-> ip ospf extlsdb-limit 25
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf](#)

Displays OSPF status and general configuration parameters.

MIB Objects

ospfGeneralGroup
ospfExtLsdbLimit

ip ospf host

Creates and deletes an OSPF entry for directly attached hosts. Allows for the modification of the host parameters of Type of Service (ToS) and metric.

ip ospf host *ip_address* **tos** *tos* [**metric** *metric*]

no ip ospf host *ip_address* **tos** *tos*

Syntax Definitions

<i>ip_address</i>	The 32-bit IP address in dotted decimal format of the OSPF host. See the example below for more information.
<i>tos</i>	The type of service (ToS) of the specified OSPF host. The valid range is 0- 15. Only ToS value 0 is supported at this time.
<i>metric</i>	The cost metric value assigned to the specified host. The valid range is 0 and up.

Defaults

parameter	default
<i>metric</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **no** variant of this command removes the record of the OSPF host.
- Use this command when multiple paths exist to a host. The specified host must be directly attached to the router. ToS routing is the ability to make a forwarding decision based on a destination address and a desired Quality of Service (QoS). ToS routing allows link selection based on QoS when more than one path exists between a source and a destination. A metric value is the cost of all the hops necessary for a packet to reach its destination. Routers use the metric to determine the best possible path.

Examples

```
-> ip ospf host 172.22.2.115 tos 1 metric 10
-> no ip ospf host 172.22.2.115 tos 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf host

Displays information on configured OSPF hosts.

MIB Objects

ospfHostTable

ospfHostStatus

ospfHostIpAddress

ospfHostTOS

ospfHostMetric

ip ospf mtu-checking

Enables or disables the use of Maximum Transfer Unit (MTU) checking. The MTU limits the size of a transmitted or received packet.

ip ospf mtu-checking

no ip ospf mtu-checking

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **no** form of this command disables MTU checking.
- This command is used to disable the checking for mismatch of the interface MTU while establishing a neighbor adjacency with a router. MTU mismatch occurs when a router receives packets that contain a larger MTU value than that of the interface on which adjacency is being established. The interface MTU is the largest IP datagram size (in bytes) that the interface can accept.

Examples

```
-> ip ospf mtu-checking
-> no ip ospf mtu-checking
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf Displays the OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf
  alaOspfMTUCheck
```

ip ospf default-originate

Configures a default external route into the OSPF routing domain.

ip ospf default-originate {only | always} [metric-type {type1 | type2}] [metric *value*]

no ip ospf default-originate

Syntax Definitions

only	Advertises only when there is a default route in the routing table.
always	Advertises the default route regardless of whether the routing table has a default route.
type1	Sets the external route as type1.
type2	Sets the external route as type2.
<i>value</i>	The metric value. The valid range is 1-65535.

Defaults

parameter	default
type1 type2	type2
<i>value</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of the command to delete redistributed default routes.

Examples

```
-> ip ospf default-originate always
-> ip ospf default-originate only metric 10
-> ip ospf default-originate always metric-type type1 metric 5
-> no ip ospf default-originate
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf asbr

Configures the router as an Autonomous System Border Router (ASBR). *This command is currently not supported.*

MIB Objects

```
alaProtocolOspf  
  alaOspfDefaultOriginate  
  alaOspfDefaultOriginateMetricType  
  alaOspfDefaultOriginateMetric
```

ip ospf route-tag

Configures a tag value for the Autonomous System External (ASE) routes created.

ip ospf route-tag *tag*

Syntax Definitions

tag The set tag value. The valid range is 0–2,147,483,647.

Defaults

parameter	default
<i>tag</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows you to set a tag value for ASE routes that are learned by this OSPF router. The tag value allows for quick identification.
- OSPF ASE route advertisements contain a tag value field. This field allows the exchange of information between autonomous system border routers (ASBRs).

Example

```
-> ip ospf route-tag 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf](#) Displays OSPF status and general configuration parameters.

MIB Objects

alaProtocolOspf
alaOspfRedistRouteTag

ip ospf spf-timer

Configures timers for Shortest Path First (SPF) calculation.

```
ip ospf spf-timer [delay delay_seconds] [hold hold_seconds]
```

Syntax Definitions

delay_seconds Specifies time (from 0 to 65535 seconds) between the reception of an OSPF topology change and the start of an SPF calculation.

hold_seconds Specifies the minimum time (from 0 to 65535 seconds) between consecutive SPF calculations.

Defaults

parameter	default
<i>delay_seconds</i>	5
<i>hold_seconds</i>	10

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows you to configure the time between SPF calculations. Using the delay timer, you can determine how much time to postpone an SPF calculation after the router receives a topology change. Using the hold timer, you can configure the amount of time that must elapse between consecutive SPF calculations.
- Note that if either of these values is set to 0, there will be no delay in the SPF calculation. This means that SPF calculations will occur immediately upon the reception of a topology change and/or that back-to back SPF calculations can take place with no break in-between the two.

Example

```
-> ip ospf spf-timer delay 20 hold 35
```

Release History

Release 7.1.1; command was introduced.

Related Commands**show ip ospf**

Displays the OSPF status and general configuration parameters.

MIB Objects

```
alaProtocolOspf  
  alaOspfTimerSpfDelay  
  alaOspfTimerSpfHold
```

ip ospf virtual-link

Creates or deletes a virtual link. A virtual link is used to restore backbone connectivity if the backbone is not physically contiguous.

```
ip ospf virtual-link area_id router_id [auth-type {none | simple | md5}] [auth-key key_string]  
[dead-interval seconds] [hello-interval seconds] [retrans-interval seconds] [transit-delay seconds]
```

```
no ip ospf virtual-link area_id router_id
```

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
<i>router_id</i>	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
none	Sets the virtual link authorization type to no authentication.
simple	Sets the virtual link authorization type to simple authentication. If simple is selected, a key must be specified as well.
md5	Sets the virtual link authorization type to MD5 authentication.
<i>key_string</i>	Sets the virtual link authorization key. The key can be up to 8 ASCII characters. See the example for more details.
dead-interval <i>seconds</i>	Sets the virtual link dead interval. If no hello packets on this link for the set number of seconds have been received, the virtual neighbor is declared dead. The valid range is 1–2147483647.
hello-interval <i>seconds</i>	Sets the virtual link hello interval, which is the time interval between OSPF hellos sent on this virtual link. The valid range is 1–65535.
retrans-interval <i>seconds</i>	Sets the virtual link retransmit interval. The router waits the set number of seconds before retransmitting OSPF packets. The valid range is 0–3600.
transit-delay <i>seconds</i>	Sets the virtual link transit delay, which is the number of seconds to transmit OSPF packets over this link. The valid range is 0–3600.

Defaults

parameter	default
none simple md5	none
<i>key_string</i>	null string
dead-interval <i>seconds</i>	40
hello-interval <i>seconds</i>	10
retrans-interval <i>seconds</i>	5
transit-delay <i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **no** form of the command deletes the virtual link.
- It is possible to define areas in such a way that the backbone is no longer contiguous. In this case the system administrator can ensure backbone connectivity physically.
- Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.
- If authentication is enabled, both routers at either end of the virtual link must share the same password. Simple authentication refers to the use of only clear-text passwords as an authentication method. MD5 authentication refers to the usage of message digests.
- The **dead-interval** value should be the same for all routers on the same network. This value should be some multiple of the value given for the hello interval.

Examples

```
-> ip ospf virtual-link 0.0.0.1 172.22.2.115
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 auth-key "techpubs"
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 auth-type simple
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 dead-interval 50
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 hello-interval 20
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 retrans-interval 20
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 transit-delay 50
-> no ip ospf virtual-link 0.0.0.1 172.22.2.115
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf virtual-link Displays the virtual link information.

MIB Objects

```
ospfVirtIfTable
  ospfVirtIfAreaId
  ospfVirtIfNeighbor
  ospfVirtIfAuthKey
  ospfVirtIfStatus
  ospfVirtIfAuthType
  ospfVirtIfRtrDeadInterval
  ospfVirtIfHelloInterval
  ospfVirtIfRetransInterval
  ospfVirtIfTransitDelay
```

ip ospf neighbor

Creates a static neighbor on a non-broadcast interface.

ip ospf neighbor *neighbor_id* {**eligible** | **non-eligible**}

no ip ospf neighbor *neighbor_id*

Syntax Definitions

neighbor_id A unique 32-bit IP address identical to the neighbor's interface address.

eligible Sets this router as eligible to be the DR.

non-eligible Sets this router as not eligible to be the DR.

Defaults

parameter	default
eligible non-eligible	eligible

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- NBMA (Non Broadcast Multi Access), PMP (Point-to-Multipoint), and P2P (Point-to-Point) OSPF non-broadcast modes are supported over Ethernet interfaces (broadcast media).
- Neighboring routers on non-broadcast OSPF networks must be statically configured, because lack of OSPF multicast capabilities prevents using normal OSPF Hello protocol discovery.
- In the case of NBMA interface the static neighbor eligibility for becoming a DR can be configured while it is not necessary for point-to-multipoint and point-to-point interfaces.
- An interface connected to this neighbor must also be configured as a non-broadcast interface, which can be either point-to-multipoint or point-to-point, by using the [ip ospf interface type](#) command.
- For the correct working of an OSPF NBMA network, a fully meshed network is mandatory. Also, the neighbor eligibility configuration for a router on every other router should match the routers interface priority configuration.

Examples

```
-> ip ospf neighbor 1.1.1.1 non-eligible
-> no ip ospf neighbor 1.1.1.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf interface type](#)

Configures the OSPF interface type.

[show ip ospf neighbor](#)

Displays information on OSPF non-virtual neighbor routers.

MIB Objects

ospfNbrTable

ospfNbrPriority

ospfNbmaNbrStatus

ip ospf area

Assigns an OSPF interface to a specified area.

ip ospf area *area_id* [summary {enable | disable}] | [type {normal | stub | nssa}]

no ip ospf area *area_id*

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
enable	Enables summarization.
disable	Disables summarization.
normal	Sets the area as a regular OSPF area.
stub	Configures an OSPF area as a stub area.
nssa	Configures an OSPF area as a Not So Stubby Area (NSSA)

Defaults

parameter	default
enable disable	enable
normal stub nssa	normal

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **no** form deletes the area.
- The **summary** options are used to enable or disable route summarization for stub and NSSA areas. Stub and NSSA areas will not receive LSA type 3 unless summary is enabled.
- The **type** command allows you to chose what type of area this is going to be.

Examples

```
-> ip ospf area 0.0.0.1
-> ip ospf area 0.0.0.1 type stub
-> ip ospf area 0.0.0.1 type normal
-> no ip ospf area 0.0.0.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area default-metric	Creates or deletes an OSPF default metric.
ip ospf area range	Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
show ip ospf area	Displays either all OSPF areas, or a specified OSPF area.

MIB Objects

```
ospfAreaTable  
  ospfImportAsExtern  
  ospfAreaSummary  
  ospfAreaId
```

ip ospf area default-metric

Creates or deletes a default metric for stub or Not So Stubby Area (NSSA) areas. The default metric configures the type of cost metric that a default area border router (ABR) will advertise in the default summary Link State Advertisement (LSA).

ip ospf area *area_id* default-metric *tos* [[cost *cost*] | [type {ospf | type 1 | type 2}]

no ip ospf area *area_id* default-metric *tos*

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
<i>tos</i>	Type of service. The valid range is 0–15. Only ToS value 0 is supported at this time.
<i>cost</i>	The numerical cost of this area and ToS. Only 0 is supported in the current release.
ospf	Advertises external routes as OSPF autonomous system external (ASE) routes.
type1	Advertises external routes as a Type 1 (non-OSPF) metric.
type2	Advertises external routes as a Type 2 (calculated weight value from non-OSPF protocol) metric.

Defaults

parameter	default
<i>tos</i>	0
ospf type 1 type 2	ospf

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **no** form deletes the default metric from the specified area.
- The **type** command configures the type of cost metric for the specified ToS. To ensure that internal routers receiving external route advertisements choose the correct route, all border routers advertising a particular external network should be configured to advertise the route using the same metric type. That is, they must all advertise the route using an OSPF, Type 1, or Type 2 metric.

Examples

```
-> ip ospf area 1.1.1.1 default-metric 0
-> no ip ospf area 1.1.1.1 default-metric 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf area](#)

Creates or deletes an OSPF area.

[ip ospf area range](#)

Creates a route summarization instance whereby a range of addresses will be advertised as a single route.

[show ip ospf area](#)

Displays either all OSPF areas, or a specified OSPF area.

MIB Objects

```
ospfStubAreaTable  
  ospfStubAreaId  
  ospfStubTOS  
  ospfStubStatus  
  ospfStubMetric  
  ospfStubMetricType
```

ip ospf area range

Creates a route summarization instance whereby a range of addresses assigned for the route at the area border router will be advertised.

```
ip ospf area area_id range {summary | nssa} ip_address subnet_mask
[effect {admatching | noMatching}]
```

```
no ip ospf area area_id range {summary | nssa} ip_address subnet_mask
```

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
summary	Advertises the address range as a summary link state advertisement (LSA).
nssa	Advertises the address range of Not So Stubby Area (NSSA) routes as a Type 5 advertisement.
<i>ip_address</i>	A 32-bit IP address for the range's area.
<i>subnet_mask</i>	A 32-bit subnet mask that determines how many bits of the IP address denote the network number.
admatching	Determines that routes specified falling within the specified range will be advertised.
noMatching	Determines that any route falling within the specified range will not be advertised.

Defaults

parameter	default
summary nssa	summary
admatching noMatching	admatching

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Route summarization is the consolidation of addresses within an area which are advertised as a single route. When network numbers in an area are assigned consecutively, the area border router can be configured, using this command, to advertise a route that aggregates all the individual networks within the range.
- Using this command causes a single route to be advertised, for an address range in the specified area, to other areas.

- An NSSA (Not So Stubby Area) is similar to a stub area. However, where autonomous system (AS) external routes cannot be imported into a stub area, an NSSA will allow the importing of some AS external routes.
- Area ranges, once created, are enabled by default. Classless Inter-Domain Routing (CIDR) can work with OSPF to make route summarization more efficient. This is especially true for the summarization of routes in the global database. OSPF area address ranges can be configured on area border routers

Examples

```
-> ip ospf area 1.1.1.1 range summary 172.22.2.0 255.255.255.0  
-> no ip ospf area 1.1.1.1 range summary 172.22.2.0 255.255.255.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area.
ip ospf area default-metric	Creates or deletes an OSPF default metric.
show ip ospf area range	Displays all or specified route summaries in a given area.

MIB Objects

```
ospfAreaAggregateTable  
  ospfAreaAggregateAreaId  
  ospfAreaAggregateLsdbType  
  ospfAreaAggregateNet  
  ospfAreaAggregateMask  
  ospfAreaAggregateEffect  
  ospfAreaAggregateStatus
```

ip ospf interface

Creates and deletes an OSPF interface.

ip ospf interface {*interface_name*}

no ip ospf interface {*interface_name*}

Syntax Definitions

interface_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to delete an OSPF interface.
- The interface name cannot contain spaces.

Examples

```
-> ip ospf interface vlan-101  
-> no ip ospf interface vlan-101
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable  
  ospfIfIpAddress  
alaOspfIfAugTable  
  alaOspfIfIntfName
```

ip ospf interface admin-state

Enables or disables the administrative status on an OSPF interface.

```
ip ospf interface {interface_name} admin-state {enable | disable}
```

```
no ip ospf interface {interface_name} admin-state {enable | disable}
```

Syntax Definitions

<i>interface_name</i>	The name of the interface.
enable	Enables the OSPF interface.
disable	Disables the OSPF interface.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to delete an OSPF interface.
- The OSPF interface must be enabled for it to participate in the OSPF protocol.

Examples

```
-> ip ospf interface vlan-101 admin-state enable
-> ip ospf interface vlan-101 admin-state disable
-> no ip ospf interface vlan-101 admin-state enable
-> no ip ospf interface vlan-101 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable
ospfIfAdminStat

ip ospf interface area

Configures an OSPF area identifier for this interface.

```
ip ospf interface {interface_name} area area_id
```

Syntax Definitions

<i>interface_name</i>	The name of the interface.
<i>area_id</i>	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

An interface must be assigned to an area to become operational.

Examples

```
-> ip ospf interface vlan-101 area 0.0.0.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf area	Displays either all the OSPF areas, or a specified OSPF area.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable
ospfIfAreaId

ip ospf interface auth-key

Configures an OSPF authentication key for simple authentication on an interface.

```
ip ospf interface {interface_name} auth-key key_string
```

Syntax Definitions

<i>interface_name</i>	The name of the interface.
<i>key_string</i>	An authentication key (8 characters maximum).

Defaults

The default for the authentication key string is a null string.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Sets a password as a simple text string of 8 ASCII characters.
- Must be used in conjunction with the **auth-type** command, described on [page 20-31](#), set to **simple**.

Examples

```
-> ip ospf interface vlan-101 auth-key pass
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface auth-type	Sets the authentication type.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable  
  ospfIfAuthKey
```

ip ospf interface auth-type

Sets the OSPF interface authentication type. Authentication allows the router to only respond to other routers that have the correct authentication information.

ip ospf interface {*interface_name*} **auth-type** [**none** | **simple** | **md5**]

Syntax Definitions

<i>interface_name</i>	The name of the interface.
none	No authentication.
simple	Simple, clear text authentication.
md5	MD5 encrypted authentication.

Defaults

parameter	default
none simple md5	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to set the type of authentication that the OSPF interface uses to validate requests for route information from other OSPF neighbors on this interface.
- Simple authentication is authentication that uses only a text string as the password. The authentication type **simple** is used in conjunction with the **auth-key** keyword described, on [page 20-30](#).
- MD5 authentication is encrypted authentication that uses an encryption key string and a key identification number. Both of these are necessary as the password. The authentication type **md5** is used in conjunction with the commands described on [page 20-35](#) and [page 20-37](#). One command enables MD5 and the other sets the key identification number.

Examples

```
-> ip ospf interface vlan-101 auth-type-simple
```

Release History

Release 7.1.1; command was introduced.

Related Commands**ip ospf interface auth-key**

Sets the password for simple authentication.

show ip ospf interface

Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable

ospfIfAuthType

ip ospf interface dead-interval

Configures the OSPF interface dead interval.

```
ip ospf interface {interface_name} dead-interval seconds
```

Syntax Definitions

interface_name The name of the interface.

seconds The dead interval, in seconds. The valid range is 1–65535.

Defaults

parameter	default
<i>seconds</i> (broadcast and point-to-point)	40
<i>seconds</i> (NBMA and point-to-multi-point)	120

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This is the interval, in seconds, after which a neighbor on this interface is considered dead if no hello packets have been received from this neighbor.
- This interval should be greater than the hello interval or the multiple of the hello interval.

Examples

```
-> ip ospf interface vlan-101 dead-interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf interface hello-interval](#) Configures the OSPF interface hello interval.

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable  
ospfIfRtrDeadInterval
```

ip ospf interface hello-interval

Configures the OSPF interface hello interval.

```
ip ospf interface {interface_name} hello-interval seconds
```

Syntax Definitions

<i>interface_name</i>	The name of the interface.
<i>seconds</i>	The hello interval, in seconds. The valid range is 0–65535. A value of 0 creates a passive OSPF interface.

Defaults

parameter	default
<i>seconds</i> (broadcast and point-to-point)	10
<i>seconds</i> (NBMA and point-to-multi-point)	30

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This is the interval between two consecutive hello packets sent out on this interface.

Examples

```
-> ip ospf interface vlan-101 hello-interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable  
ospfIfHelloInterval
```

ip ospf interface md5

Creates and deletes the OSPF interface MD5 key identification number.

ip ospf interface {*interface_name*} **md5** *key_id* [**enable** | **disable**]

Syntax Definitions

<i>interface_name</i>	The name of the interface.
<i>key_id</i>	A key identification number. The key identification number specifies a number that allows MD5 encrypted routers to communicate. Both routers must use the same key ID. The valid range is 1–255.
enable	Enables the interface key.
disable	Disables the interface key.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- MD5 authentication can be used to encrypt information sent over the network. MD5 authentication works by using shared secret keys. Keys are used to sign the packets with an MD5 checksum, and they cannot be forged or tampered with. Since the keys are not included in the packet, snooping the key is not possible.
- This command is used in conjunction with the commands described on [page 20-31](#) and [page 20-37](#).
- The **no** variant deletes the key ID number.

Examples

```
-> ip ospf interface vlan-101 md5 100
-> ip ospf interface vlan-101 md5 10 disable
-> ip ospf interface vlan-101 md5 10 enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface md5 key	Configures the OSPF key ID and key.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
alaOspfIfMd5Table  
  alaOspfIfMd5IpAddress  
  alaOspfIfMd5KeyId
```

ip ospf interface md5 key

Configures the OSPF key string. This interface MD5 string, along with the key identification number, enables the interface to encode MD5 encryption.

```
ip ospf interface {interface_name} md5 key_id key key_string
```

Syntax Definitions

<i>interface_name</i>	The name of the interface.
<i>key_id</i>	The key ID. The valid range is 1–255.
<i>key_string</i>	A key string.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used in conjunction with the commands described above on [page 20-31](#) and [page 20-35](#).
- For MD5 authentication to function properly the same key string must be configured on the neighboring router for that interface.

Examples

```
-> ip ospf interface vlan-101 md5 100 key 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface md5	Creates and deletes the OSPF interface MD5 key identification number.
show ip ospf interface	Displays the status and statistics of an OSPF interface.

MIB Objects

```
alaOspfIfMd5Table  
  alaOspfIfMd5IpAddress  
  alaOspfIfMd5KeyId  
  alaOspfIfMd5Key
```

ip ospf interface type

Configures the OSPF interface type.

ip ospf interface {*interface_name*} **type** {**point-to-point** | **point-to-multipoint** | **broadcast** | **non-broadcast**}

Syntax Definitions

<i>interface_name</i>	The name of the interface.
point-to-point	Sets the interface to be a point-to-point OSPF interface.
point-to-multipoint	Sets the interface to be a point-to-multipoint OSPF interface.
broadcast	Sets the interface to be a broadcast OSPF interface.
non-broadcast	Sets the interface to be NBMA (Non Broadcast Multi Access) OSPF interface.

Defaults

parameter	default
broadcast non-broadcast point-to-point point-to-multipoint	broadcast

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command sets an interface to be broadcast, non-broadcast, point-to-point, or point-to-multipoint.
- If the type is non-broadcast or point-to-multipoint, static neighbors should be configured.

Examples

```
-> ip ospf interface vlan-101 type non-broadcast
```

Release History

Release 7.1.1; command was introduced.

Related Commands**ip ospf neighbor**

Creates a static neighbor on a Non Broadcast Multi Access (NBMA) interface.

show ip ospf interface

Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable

ospfIfType

ip ospf interface cost

Configures the OSPF interface cost.

```
ip ospf interface {interface_name} cost cost
```

Syntax Definitions

interface_name The name of the interface.

cost The interface cost. The valid range is 0 to 65535.

Defaults

parameter	default
<i>cost</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The configured interface cost, if any, is used during OSPF route calculations.

Examples

```
-> ip ospf interface vlan-101 cost 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfMetricTable  
  ospfIfMetricIpAddress  
  ospfIfMetricValue
```

ip ospf interface poll-interval

Configures the OSPF poll interval for a Non Broadcast Multi Access (NBMA) interface.

```
ip ospf interface {interface_name} poll-interval seconds
```

Syntax Definitions

interface_name The name of the interface.

seconds The poll interval, in seconds. The valid range is 1–2147483647.

Defaults

parameter	default
<i>seconds</i>	120

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This parameter configures the larger time interval, in seconds, between hello packets sent to an inactive neighbor.

Examples

```
-> ip ospf interface vlan-101 poll-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

```
ospfIfTable  
ospfIfPollInterval
```

ip ospf interface priority

Configures the OSPF interface priority. The priority number helps determine the eligibility of this router to become the designated router on the network.

```
ip ospf interface {interface_name} priority priority
```

Syntax Definitions

interface_name The name of the interface.

priority The interface priority. The valid range is 0–255.

Defaults

parameter	default
<i>priority</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the highest priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become the designated router.

Examples

```
-> ip ospf interface vlan-101 priority 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable
ospfIfRtrPriority

ip ospf interface retrans-interval

Configures the OSPF interface retransmit interval.

```
ip ospf interface {interface_name} retrans-interval seconds
```

Syntax Definitions

interface_name The name of the interface.

seconds The retransmit interval, in seconds. The valid range 0–3600.

Defaults

parameter	default
<i>seconds</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The number of seconds between link retransmission of OSPF packets on this interface.

Examples

```
-> ip ospf interface vlan-101 retrans-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable
ospfIfRetransInterval

ip ospf interface transit-delay

Configures the OSPF interface transit delay.

```
ip ospf interface {interface_name} transit-delay seconds
```

Syntax Definitions

interface_name The name of the interface.

seconds The transit delay, in seconds. The valid range is 0–3600.

Defaults

parameter	default
<i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The estimated number of seconds required to transmit a link state update over this interface. This command takes into account transmission and propagation delays and must be greater than 0.

Examples

```
-> ip ospf interface vlan-101 transit-delay 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf interface](#) Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable
ospfIfTransitDelay

ip ospf restart-support

Configures support for the graceful restart feature on an OSPF router.

ip ospf restart-support {planned-unplanned | planned-only}

no ip ospf restart-support

Syntax Definitions

planned-unplanned Specifies support for planned and unplanned restarts.

planned-only This parameter is currently not supported.

Defaults

Graceful restart is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to disable support for the graceful restart feature on an OSPF router.
- The minimum hardware configuration for this command is a redundant CMM configuration.

Examples

```
-> ip ospf restart-support planned-unplanned
-> no ip ospf restart-support
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf restart Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
  alaOspfRestartSupport
```

ip ospf restart-interval

Configures the grace period for achieving a graceful OSPF restart.

ip ospf restart-interval [*seconds*]

Syntax Definitions

seconds The hitless restart timeout interval, in seconds. The valid range is 0–1800.

Defaults

parameter	default
<i>seconds</i>	120

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 10K switches with a single CMM.

Example

```
-> ip ospf restart-interval 600
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf restart-support](#) Administratively enables and disables support for the graceful restart feature on an OSPF router.

[show ip ospf restart](#) Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf  
  alaOspfRestartInterval
```

ip ospf restart-helper admin-state

Administratively enables and disables the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart.

ip ospf restart-helper [admin-state {enable | disable}]

Syntax Definitions

enable	Enables the capability of an OSPF router to operate in helper mode.
disable	Disables the capability of an OSPF router to operate in helper mode.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 10K switches with a single CMM.

Examples

```
-> ip ospf restart-helper admin-state disable
-> ip ospf restart-helper admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.
ip ospf restart-helper strict-lsa-checking admin-state	Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.
show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf
  alaOspfRestartHelperSupport
```

ip ospf restart-helper strict-lsa-checking admin-state

Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

ip ospf restart-helper strict-lsa-checking admin-state {enable | disable}

Syntax Definitions

enable	Enables whether or not a changed LSA will result in termination of graceful restart by a helping router.
disable	Disables whether or not a changed LSA will result in termination of graceful restart by a helping router.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 10K switches with a single CMM.

Examples

```
-> ip ospf restart-helper strict-lsa-checking admin-state disable  
-> ip ospf restart-helper strict-lsa-checking admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf restart-support	Administratively enables and disables support for the graceful restart feature on an OSPF router.
ip ospf restart-helper admin-state	Administratively enables and disables the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart.
show ip ospf restart	Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf  
  alaOspfRestartHelperSupport
```

ip ospf restart initiate

Initiates a planned graceful restart.

ip ospf restart initiate

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You must execute this command on the primary CMM before executing a **takeover** command.
- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 10K switches with a single CMM.

Example

```
-> ip ospf restart initiate
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf restart](#) Displays the OSPF graceful restart related configuration and status.

MIB Objects

```
alaProtocolOspf  
  alaOspfRestartInitiate
```

show ip ospf

Displays the OSPF status and general configuration parameters.

show ip ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display the general configuration parameters of the OSPF router.
- See the Related Commands section below to modify the displayed parameters.

Examples

```
-> show ip ospf
```

```
Router Id                = 10.255.11.242,
OSPF Version Number      = 2,
Admin Status             = Enabled,
Area Border Router?     = No,
AS Border Router Status  = Disabled,
Route Redistribution Status = Disabled,
Route Tag                 = 0,
SPF Hold Time (in seconds) = 10,
SPF Delay Time (in seconds) = 5,
MTU Checking             = Disabled,
# of Routes              = 0,
# of AS-External LSAs    = 0,
# of self-originated LSAs = 0,
# of LSAs received       = 0,
External LSDB Limit      = -1,
Exit Overflow Interval   = 0,
# of SPF calculations done = 0,
# of Incr SPF calculations done = 0,
# of Init State Nbrs     = 0,
# of 2-Way State Nbrs    = 0,
# of Exchange State Nbrs = 0,
# of Full State Nbrs     = 0,
# of attached areas      = 1,
# of Active areas        = 0,
# of Transit areas       = 0,
# of attached NSSAs      = 0
```


output definitions

Router Id	The unique identification for the router.
OSPF Version Number	The version of OSPF the router is running.
Admin Status	Whether OSPF is currently enabled or disabled on the router.
Area Border Router?	Whether the router status is an area router or not.
AS Border Router Status	Whether the area Autonomous System Border Router status of this router is enabled or disabled.
Route Redistribution Status	Whether route redistribution is enabled or disabled on the router. This is set using the ip ospf default-originate command.
Route Tag	Shows the route tag for this router.
SPF Hold Time	Shows the time in seconds between the reception of an OSPF topology change and the start of a SPF calculation.
SPF Delay Time	Shows the time in seconds between consecutive SPF calculations.
MTU Checking	Shows whether Maximum Transfer Unit checking is enabled or disabled. This is set using the ip ospf mtu-checking command.
# of routes	The total number of OSPF routes known to this router.
# of AS-External LSAs	The number of external routes learned from outside the router's Autonomous System (AS).
# of self-originated LSAs	The number of times a new Link State Advertisement has been sent from this router.
# of LSAs received	The number of times a new Link State Advertisement has been received by this router.
External LSDB Limit	The maximum number of entries allowed in the external Link State Database.
Exit Overflow Interval	The number of seconds the router remains in the overflow state before attempting to leave it. This is set using the ip ospf exit-overflow-interval command.
# of SPF calculations done	The number of SPF calculations that have occurred.
# of Incr SPF calculations done	The number of incremental SPF calculations done.
# of Init State Nbrs	The number of neighbors in the initialization state.
# of 2-Way State Nbrs	The number of OSPF 2-way state neighbors on this router.
# of Exchange State Nbrs	The number of neighbors in the exchange state.
# of Full State Nbrs	The number of neighbors in the full state.
# of attached areas	The number of areas that are configured on the router.
# of Active areas	The number of areas that are active.
# of Transit areas	The number of transit areas that are configured on the router.
# of attached NSSAs	The number of Not So Stubby Areas that are configured on the router.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf admin-state	Enables or disables the administration of OSPF on the router.
ip ospf mtu-checking	Enables or disables the use of Maximum Transfer Unit (MTU) checking.
ip ospf spf-timer	Configures timers for SPF calculation.
ip ospf default-originate	Enables or disables OSPF redistribution
ip ospf asbr	Configures the router as an Autonomous System Border Router (ASBR). <i>This command is currently not supported.</i>
ip ospf extlsdb-limit	Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.
ip ospf exit-overflow-interval	This command sets the overflow interval value.
ip ospf route-tag	Configures a tag value for Autonomous System External (ASE) routes created.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
ospfGeneralGroup
  ospfRouterId
  ospfAdminStat
  ospfVersionNumber
  ospfAreaBdrRtrStatus
  ospfASBdrRtrStatus
  ospfExternLsaCount
  ospfExternLsaCksumSum
  ospfTOSsupport
  ospfOriginateNewLsas
  ospfRxNewLsas
  ospfExtLsdbLimit
  ospfExitOverflowInterval
alcatelIND1Ospf
  alaOspfRedistAdminStatus
  alaOspfRedistRouteTag
  alaOspfTimerSpfDelay
  alaOspfTimerSpfHold
  alaOspfRouteNumber
  alaOspfMTUcheck
```

show ip ospf border-routers

Displays information regarding all or specified border routers.

show ip ospf border-routers [*area_id*] [*router_id*] [*tos*] [*gateway*]

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
<i>router_id</i>	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
<i>tos</i>	The Type of Service. The valid range is 0–15. Only ToS value 0 is supported at this time.
<i>gateway</i>	The 32-bit IP address of the gateway for the border router being displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display a list of border routers known by this OSPF router.
- By using the optional parameters, you can display the border routers using the specified parameter. For example, to find a router using a router ID of 1.1.1.1, enter the command using the router ID of 1.1.1.1 as a search criteria.
- See the related commands sections below to modify the list.

Examples

```
-> show ip ospf border-routers 10.0.0.0
```

Router Id	Area Id	Gateway	TOS	Metric
10.0.0.0	1.0.0.1	143.209.92.71	1	1

output definitions

Router ID	The unique identification for the router.
Area ID	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
Gateway	The next hop interface on which the border router has been learned.
ToS	The Type of Service. Only ToS value 0 is supported at this time.
Metric	The cost to the border router.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaOspfBdrRouterAreaId  
alaOspfBdrRouterId  
alaOspfBdrRouterTos  
alaOspfBdrRouterMetric
```

show ip ospf ext-lsdb

Displays external Link State Advertisements known by this router.

```
show ip ospf ext-lsdb [linkstate-id ls_id] [router-id router_id]
```

Syntax Definitions

<i>ls_id</i>	The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.
<i>router_id</i>	The Router ID. The ID is a unique 32-bit value such as an IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display the external link state database (LSDB) for the OSPF router.
- This command can be used for OSPF debugging purposes, specifically to narrow down sections of attached areas to determine which sections are receiving the specified external LSAs. You may specify only the parameters from the area LSDB in which you are interested using the optional command parameters.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf ext-lsdb
```

LS Id	Orig Router-Id	SeqNo	Age	Protocol
198.168.100.100	198.168.100.100	10	100	STATIC

output definitions

LS Id	The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.
Orig Router-Id	The router ID of the router that originated the external LSDB.
SeqNo	The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).
Age	The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.
Protocol	The type of protocol, if any.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf extlsdb-limit](#)

Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.

MIB Objects

ospfExtLsdbTable

ospfExtLsdbLsid

ospfExtLsdbRouterId

ospfExtLsdbSequence

ospfExtLsdbAge

ospfExtLsdbType

show ip ospf host

Displays information on the configured OSPF hosts.

show ip ospf host [*ip_address*]

Syntax Definitions

ip_address A 32-bit IP address for a directly attached host.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display general information for OSPF hosts directly attached to this router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf host 172.22.2.115
```

Host Address	TOS	Metric	Status	AreaId
143.209.92.12	1	0	Up	0.0.0.0

output definitions

Host Address	A 32-bit IP address for a directly attached host. This can be set using the ip ospf host command.
ToS	The Type of Service traffic from the host is labeled as. ToS is set using the ip ospf host command.
Metric	The metric assigned to the host. Metric is set using the ip ospf host command.
Status	Whether the host is enabled or disabled.
AreaId	The area identification for the host's area.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf host](#)

Creates and deletes an OSPF entry for directly attached hosts.

MIB Objects

ospfHostTable

ospfHostIpAddress

ospfHostTOS

ospfHostMetric

ospfHostStatus

ospfHostAreaID

show ip ospf lsdb

Displays LSAs in the Link State Database associated with each area.

```
show ip ospf lsdb [area_id] [rtr | net | netsum | asbrsum] [linkstate-id ls_id] [router-id router_id]
```

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
rtr	Specifies router LSAs.
net	Specifies network LSAs.
netsum	Specifies network summary LSAs.
asbrsum	Specifies Autonomous System Border Router summary LSAs.
<i>ls_id</i>	The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.
<i>router_id</i>	The Router ID. The ID is a unique 32-bit value such as an IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display the Link State Database (LSDB) of the OSPF router. This command can be used for OSPF debugging purposes, specifically to narrow down sections of an area to determine which sections are receiving the specified link state advertisements. You may specify only the parameters from the area LSDB in which you are interested using the optional command parameters.
- You can view link state advertisements by specifying either a link state identifier or a router identifier. However, when specifying a router ID, you must also supply a valid link state ID.

Examples

```
-> show ip ospf lsdb
  Area Id      Type      LS Id      Orig Router-Id  SeqNo      Age
-----+-----+-----+-----+-----+-----
0.0.0.1      OSPF      198.168.100.100  198.168.100.100  1          100
```

output definitions

Area Id	The area identification for the area to which the record belongs.
Type	The protocol type from where the route was learned.
LS Id	The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.

output definitions (continued)

Orig Router-Id	The router ID of the router that originated the external LSDB.
SeqNo	The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).
Age	The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf](#) Displays the OSPF status and general configuration parameters.

MIB Objects

ospfLsdbTable
 ospfLsdbAreaId
 ospfLsdbType
 ospfLsdbLsid
 ospfLsdbRouterId
 ospfLsdbSequence
 ospfLsdbAge

show ip ospf neighbor

Displays information on OSPF non-virtual neighbor routers.

```
show ip ospf neighbor [ip_address]
```

Syntax Definitions

ip_address A 32-bit IP address of the neighboring router.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display all non-virtual neighbors of the OSPF router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf neighbor
```

IP Address	Area Id	Router Id	Vlan	State	Mode
1.1.1.1	255.255.255.255	0.0.0.0	0	Down	Static

output definitions

IP Address	The IP address of the neighbor.
Area Id	A unique 32-bit value, such as an IP address, that identifies the neighboring router in the Autonomous System.
Router Id	The unique identification for the neighboring router.
VlanId	The VLAN corresponding to this interface on which the neighbor is reachable.
State	The state of the OSPF neighbor adjacency.
Mode	What type of neighbor, either Dynamic (learned) or Static .

```

-> show ip ospf neighbor 1.1.1.1
Neighbor's IP Address           = 1.1.1.1,
Neighbor's Router Id           = 0.0.0.0,
Neighbor's Area Id             = 255.255.255.255,
Neighbor's DR Address          = 0.0.0.0,
Neighbor's BDR Address         = 0.0.0.0,
Neighbor's Priority             = 1,
Neighbor's State               = Down,
Hello Suppressed ?             = No,
Neighbor's type                = Static,
DR Eligible                    = Yes,
# of State Events              = 0,
Mode                           = Slave,
MD5 Sequence Number           = 0,
Time since Last Hello          = 0 sec,
# of Outstanding LS Requests   = 0,
# of Outstanding LS Acknowledgements = 0,
# of Outstanding LS Retransmissions = 0,
Restart Helper Status          = Not Restarting,
Restart Age (in seconds)       = 0 sec,
Last Restart Helper Exit Reason = None

```

output definitions

Neighbor's IP Address	The IP address of the neighbor.
Neighbor's Router Id	The identification number for the selected host's record. It is most often the router's IP address.
Neighbor's Area Id	Identifier of the OSPF Area to which the neighbor is attached. 255.255.255.255 shows that this neighbor is not attached to any area.
Neighbor's DR Address	The address of the neighbors Designated Router.
Neighbor's BDR Address	The address of the neighbors Backup Designated Router.
Neighbor's Priority	The priority value for this neighbor becoming the DR.
Neighbor's State	The condition of the OSPF neighbor's state machine.
Hello Suppressed	Whether sending hello messages to this neighbor is suppressed.
Neighbor's type	What type of neighbor this is, either dynamic or static.
DR Eligible	Shows the eligibility status of the static neighbor. If it is configured as "ineligible" during creation of the neighbor, it shows up as No . Otherwise, if configured as Eligible (the default), it shows up as Yes .
# of State Events	The number of state events restricted for this neighbor and the local router.
Mode	The role the neighbor has with the local router during DD Exchange, which can be Master or Slave.
MD5 Sequence Number	The sequence number of the MD5 authorization key.
Time since Last Hello	The amount of time (in seconds) since the last HELLO messages was received from this neighbor.
# of Outstanding LS Requests	The number of Link State requests to this neighbor that have not received a response from this neighbor.
# of Outstanding LS Acknowledgements	Number of Link state Acknowledgements queued up by the local router to be sent to the neighbor.

output definitions (continued)

# of Outstanding LS Retransmissions	The number of Link State updates to the neighbor that need to be retransmitted by the OSPF router.
Restart Helper Status	Indicates whether the router is acting as a hitless restart helper for the neighbor.
Restart Age	The remaining time, in seconds, for the current OSPF hitless restart interval if the router is acting as a restart helper for the neighbor.
Last Restart Helper Exit Reason	The outcome of the last attempt at acting as a hitless restart helper for the neighbor.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf neighbor](#) Creates a static neighbor on a Non Broadcast Multi Access (NBMA) interface.

MIB Objects

```
ospfNbrTable
  ospfNbrIpAddr
  ospfNbrRtrId
  ospfNbrOptions
  ospfNbrPriority
  ospfNbrState
  ospfNbrEvents
  ospfNbrHelloSuppressed
alaOspfNbrAugTable
  alaOspfNbrRestartHelperStatus
  alaOspfNbrRestartHelperAge
  alaOspfNbrRestartHelperExitReason
```

show ip ospf routes

Displays the OSPF routes known to the router.

show ip ospf routes [*ip_addr mask tos gateway*]

Syntax Definitions

<i>ip_addr</i>	The 32-bit IP address of the route destination in dotted decimal format.
<i>mask</i>	The IP subnet mask of the route destination.
<i>tos</i>	The Type of Service of the route.
<i>gateway</i>	The next hop IP address for this router.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If no variables are entered, all routes are displayed. If the variables are entered, then only routes matching the specified criteria are shown. All the variables described above must be entered for a route match. If all of the variables are not entered, an error message is returned.

Examples

```
-> show ip ospf routes
```

```

Destination/Mask      Gateway      Metric  Vlan  Type
-----+-----+-----+----+-----
198.168.100.100      195.5.2.8   0       5     AS-Ext

```

output definitions

Destination/Mask	The destination address of the route. This can also display the destination IP address mask if it is known.
Gateway	The gateway address of the route.
Metric	The cost of the route.
Vlan	The VLAN number on which the gateway can be routed.
Type	The type of OSPF route.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip ospf](#)

Displays the OSPF status and general configuration parameters.

MIB Objects

AlcatellINDospf

alaOspfRouteDest

alaOspfRouteMask

alaOspfRouteNextHop

alaOspfRouteMetric1

show ip ospf virtual-link

Displays virtual link information. A virtual link is used to connect OSPF backbone routers that are not physically contiguous.

show ip ospf virtual-link [*router_id*]

Syntax Definitions

router_id The router ID of the remote end of the virtual link that is to be viewed.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf virtual-link
```

```

                                State
  Transit AreaId      Router-id   Link / Adjacency  AuthType  OperStatus
-----+-----+-----+-----+-----
1.1.1.1              172.17.1.1      P2P / Full       none      up

```

output definitions

Transit AreaId	The area identification for the area assigned to the virtual link.
Router-Id	The destination router identification for the virtual link.
State Link	The state of the virtual link with regards to the local router.
State Adjacency	The state of the virtual link adjacency.
AuthType	The type of authorization employed by the virtual link.
OperStatus	Displays whether the virtual link is enabled or disabled.

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip ospf virtual-link** Creates or deletes a virtual link.
show ip ospf virtual-neighbor Displays OSPF virtual neighbors.

MIB Objects

```
ospfVirtIfTable  
  ospfVirtIfAreaId  
  ospfVirtIfNeighbor  
  ospfVirtIfState  
  ospfVirtIfAuthType
```

show ip ospf virtual-neighbor

Displays OSPF virtual neighbors. A virtual neighbor is connected to the router through a virtual link rather than a physical one.

show ip ospf virtual-neighbor *area_id* *router_id*

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
<i>router_id</i>	A unique 32-bit value, such as an IP address, that identifies the configured OSPF area in the AS.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display all virtual neighbors for the OSPF router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ip ospf virtual-neighbor 0.0.0.0 10.0.0.1
```

AreaId	RouterId	Priority	Events	RxmtQlen	LastHello	State
0.0.0.0	10.0.0.0	1	10	100	323	INIT

output definitions

AreaId	The area identification for the area of which the virtual neighbor is a part.
RouterId	The router identification of the virtual neighbor.
Priority	The number used to determine whether the virtual neighbor will become the designated router for its area.
Events	The number of OSPF control message sent by the neighbor to the router.
RxmtQlen	The length (in number of packets) of the retransmit queue.
LastHello	The last Hello message sent by the neighbor
State	The current state the virtual neighbor is in relative to the router; this will be INIT, Exchange, or Full.

```

-> show ip ospf virtual-neighbor 0.0.0.1 2.0.0.254
Neighbor's IP Address           = 2.0.0.254,
Neighbor's Router Id           = 2.0.0.254,
Neighbor's Area Id             = 0.0.0.1,
Neighbor's DR Address          = 2.0.0.1,
Neighbor's BDR Address         = 2.0.0.254,
Neighbor's Priority             = 1,
Neighbor's State                = Full,
Hello Suppressed ?             = No,
Neighbor's type                 = Dynamic,
# of State Events              = 6,
Mode = Master,
MD5 Sequence Number            = 0,
Time since Last Hello          = 5 sec,
Last DD I_M_MS                 =
# of Outstanding LS Requests   = 0,
# of Outstanding LS Acknowledgements = 0,
# of Outstanding LS Retransmissions = 0,
Restart Helper Status          = Not Restarting,
Restart Age (in seconds)       = 0 sec,
Last Restart Helper Exit Reason = None

```

output definitions

Neighbor's IP Address	The IP address of the virtual neighbor.
Neighbor's Router Id	The identification number for the selected host's record. It is most often the router's IP address.
Neighbor's Area Id	Identifier of the OSPF Area to which the virtual neighbor is attached. 255.255.255.255 shows that this virtual neighbor is not attached to any area.
Neighbor's DR Address	The address of the virtual neighbor's Designated Router.
Neighbor's BDR Address	The address of the virtual neighbor's Backup Designated Router.
Neighbor's Priority	The priority value for this virtual neighbor becoming the DR.
Neighbor's State	The condition of the OSPF virtual neighbor's state machine.
Hello Suppressed	Whether sending hello messages to this virtual neighbor is suppressed.
Neighbor's type	What type of virtual neighbor this is, either dynamic or static.
DR Eligible	Shows the eligibility status of the virtual neighbor. If it is configured as "ineligible" during creation of the neighbor, it shows up as No . Otherwise, if configured as Eligible (the default), it shows up as Yes .
# of State Events	The number of state events restricted for this virtual neighbor and the local router.
Mode	The role the virtual neighbor has with the local router during DD Exchange, which can be Master or Slave.
MD5 Sequence Number	The sequence number of the MD5 authorization key.
Time since Last Hello	The amount of time (in seconds) since the last HELLO messages was received from this virtual neighbor.
Last DD I_M_MS	The initialize (I), more (M) and master (MS) bits, and Options field Data Description (DD) packet received from the virtual neighbor. This parameter is used to determine whether the next DD packet has been received or not.

output definitions (continued)

# of Outstanding LS Requests	The number of Link State requests to this virtual neighbor that have not received a response from this virtual neighbor.
# of Outstanding LS Acknowledgements	Number of Link state Acknowledgements queued up by the local router to be sent to the virtual neighbor.
# of Outstanding LS Retransmissions	The number of Link State updates to the virtual neighbor that need to be retransmitted by the OSPF router.
Restart Helper Status	Indicates whether the router is acting as a hitless restart helper for the virtual neighbor.
Restart Age	The remaining time, in seconds, for the current OSPF hitless restart interval if the router is acting as a restart helper for the virtual neighbor.
Last Restart Helper Exit Reason	The outcome of the last attempt at acting as a hitless restart helper for the virtual neighbor.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf virtual-link](#) Creates or deletes a virtual link.

MIB Objects

ospfVirtNbrTable

ospfVirtNbrArea
ospfVirtNbrRtrId
ospfVirtNbrState

alaOspfVirtNbrAugTable

alaOspfVirtNbrRestartHelperStatus
alaOspfVirtNbrRestartHelperAge
alaOspfVirtNbrRestartHelperExitReason

show ip ospf area

Displays either all OSPF areas, or a specified OSPF area.

show ip ospf area [*area_id*]

Syntax Definitions

area_id A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Allows you to view the details of a specified OSPF area.
- Not specifying an OSPF area will display all known areas for the OSPF router.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ip ospf area
```

Area Id	AdminStatus	Type	OperStatus
1.1.1.1	disabled	normal	down
0.0.0.1	disabled	normal	down

```
-> show ip ospf area 0.0.0.0
```

```
Area Identifier           = 1.1.1.1,
Admin Status              = Disabled,
Operational Status       = Down,
Area Type                 = normal,
Area Summary              = Enabled,
Time since last SPF Run   = 00h:00m:27s,
# of Area Border Routers known = 0,
# of AS Border Routers known = 0,
# of LSAs in area        = 0,
# of SPF Calculations done = 0,
# of Incremental SPF Calculations done = 0,
# of Neighbors in Init State = 0,
# of Neighbors in 2-Way State = 0,
# of Neighbors in Exchange State = 0,
# of Neighbors in Full State = 0,
# of Interfaces attached   = 0
Attached Interfaces        = vlan-213
```

output definitions

Area Identifier	The unique 32-bit value, such as IP address, that identifies the OSPF area in the AS.
Admin Status	Whether the area is enabled or disabled.
Operational Status	Whether the area is active.
Area Type	The area type. This field will be normal , stub , or NSSA .
Area Summary	Whether Area Summary is enabled or disabled.
Time since last SPF Run	The last time the Shortest Path First calculation was performed.
# of Area Border Routers known	The number of Area Border Routers in the area.
# of AS Border Routers known	The number of Autonomous System Border Routers in the area.
# of LSAs	The total number of Link State Advertisements for the Area.
# of SPF Calculations	The number of times the area has calculated the Shortest Path.
# of Incremental SPF Calculations	The number of incremental Shortest Path First calculations that have been performed in the area.
# of Neighbors in Init State	The number of OSPF neighbors that are in initialization.
# of Neighbors in 2-Way State	The number of OSPF 2-way state neighbors in this area.
# of Neighbors in Exchange State	The number of OSPF neighbors that are currently establishing their status.
# of Neighbors in Full State	The number of OSPF neighbors.
# of Interfaces attached	The number of OSPF interfaces.
Attached Interfaces	The names of the OSPF interfaces attached to this area.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area	Creates or deletes an OSPF area, assigning default metric, cost, and type.
ip ospf area range	Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
show ip ospf interface	Displays OSPF interface information.

MIB Objects

ospfAreaTable

ospfAreaId

ospfImportAsExtern

ospfSpfRuns

ospfAreaBdrRtrCount

ospfAsBdrRtrCount

ospfAreaLsaCount

ospfAreaSummary

ospfAreaStatus

alaOspfIfAugTable

alaOspfIfIntfName

show ip ospf area range

Displays all or specified route summaries in a given area.

```
show ip ospf area area_id range [{summary | nssa} ip_address ip_mask]
```

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
summary	Specifies that routes are summarized.
nssa	Specifies the Not So Stubby Area (NSSA) routers are summarized.
<i>ip_address</i>	A 32-bit IP address.
<i>ip_mask</i>	A 32-bit subnet mask.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Allows you to view the details of a specified OSPF area range.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ip ospf area 0.0.0.0 range
```

AreaId	Type	Destination	Advertise
0.0.0.0	Summary	192.168.12.1/24	Matching
0.0.0.0	NSSA	143.209.92.71/24	noMatching

output definitions

AreaId	The area identification for the area range.
Type	The type of area the range is associated with.
Destination	The destination address of the range.
Advertise	Shows the filter effect of the range. LSAs in the range are either advertised (Matching) or not advertised (noMatching).

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip ospf area range](#)

Creates a route summarization instance whereby a range of addresses assigned for the route at the area border router will be advertised.

MIB Objects

```
ospfAreaRangeTable  
  ospfAreaRangeAreaId  
  ospfAreaRangeNet  
  ospfAreaRangeMask  
  ospfAreaRangeStatus  
  ospfAreaRangeEffect
```

show ip ospf area stub

Displays stub default area metrics, if configured.

show ip ospf area *area_id* stub

Syntax Definitions

area_id A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip ospf area 0.0.0.1 stub
```

```

      Area Id      TOS      Metric      MetricType
-----+-----+-----+-----
0.0.0.1          1          1          ospf

```

output definitions

Area Id	The identification number of the stub area.
TOS	The Type of Service assignment.
Metric	The metric assignment of the default router in the stub area.
MetricType	The metric type of the stub area. It will be either ospf , type1 , or type2 .

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf area Creates or deletes an OSPF area.

MIB Objects

```
ospfStubAreaTable  
  ospfStubAreaId  
  ospfStubTOS  
  ospfStubMetric  
  ospfStubStatus  
  ospfStubMetricType
```

show ip ospf interface

Displays OSPF interface information.

show ip ospf interface [*interface_name*]

Syntax Definitions

interface_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Not specifying an interface name displays all known interfaces for the OSPF router.

Examples

No interface name is specified:

```
-> show ip ospf interface
```

Interface Name	DR Address	Backup DR Address	Admin Status	Oper Status	State
vlan-213	213.10.10.1	213.10.10.254	enabled	up	DR
vlan-215	215.10.10.254	215.10.10.1	enabled	up	BDR

output definitions

Interface Name	The name of the interface.
DR Address	The designated router IP address on this network segment. Make sure you configure a VLAN for the router IP. (See Chapter 4, “VLAN Management Commands,” for more information.)
Backup DR Address	The IP address of the backup designated router.
Vlan	The VLAN to which the interface is assigned.
Admin Status	The current administration status of the interface, either enabled or disabled .
Oper Status	Whether the interface is an active OSPF interface.
State	The current state of the OSPF interface. It will be down , up , dp , dr , or other .

The following is an example of MD5 authentication (an interface name is used in this example).

```
-> show ip ospf interface vlan-3
Interface IP Name           = vlan-3
VLAN Id                     = 3,
Interface IP Address        = 100.10.10.2,
Interface IP Mask           = 255.255.255.0,
Admin Status                = Enabled,
Operational Status         = Up,
OSPF Interface State       = BDR,
Interface Type              = Broadcast,
Area Id                     = 0.0.0.2,
Designated Router IP Address = 100.10.10.88,
Designated Router RouterId  = 100.10.10.88,
Backup Designated Router IP Address = 100.10.10.2,
Backup Designated Router RouterId = 192.169.1.2,
MTU (bytes)                 = 1500,
Metric Cost                 = 1,
Priority                     = 1,
Hello Interval (seconds)    = 10,
Transit Delay (seconds)     = 1,
Retrans Interval (seconds)  = 5,
Dead Interval (seconds)     = 40,
Poll Interval (seconds)     = 120,
Link Type                    = Broadcast,
Authentication Type         = md5,
#   Id   Key   Status   StartAccept   StopAccept   StartGen   StopGen
---+---+---+-----+-----+-----+-----+
1  1     Set  Enabled     0             0             0           0
# of Events                  = 2,
# of Init State Neighbors    = 0,
# of 2-Way State Neighbors   = 0,
# of Exchange State Neighbors = 0,
# of Full State Neighbors    = 1
BFD status                   = Disabled,
DR-Only Option for BFD      = Disabled
```

Note. See the table of the following page for output definitions.

The following is an example of simple authentication (an interface name is used in this example):

```
-> show ip ospf interface vlan-3
Interface IP Name           = vlan-3
VLAN Id                    = 3,
Interface IP Address       = 100.10.10.2,
Interface IP Mask          = 255.255.255.0,
Admin Status               = Enabled,
Operational Status        = Up,
OSPF Interface State      = DR,
Interface Type             = Broadcast,
Area Id                    = 0.0.0.2,
Designated Router IP Address = 100.10.10.2,
Designated Router RouterId = 192.169.1.2,
Backup Designated Router IP Address = 0.0.0.0,
Backup Designated Router RouterId = 0.0.0.0,
MTU (bytes)                = 1500,
Metric Cost                = 1,
Priority                   = 1,
Hello Interval (seconds)   = 10,
Transit Delay (seconds)    = 1,
Retrans Interval (seconds) = 5,
Dead Interval (seconds)    = 40,
Poll Interval (seconds)    = 120,
Link Type                  = Broadcast,
Authentication Type        = simple,
Authentication Key         = Set,
# of Events                 = 3,
# of Init State Neighbors  = 0,
# of Exchange State Neighbors = 0,
# of 2-Way State Neighbors = 0,
# of Full State Neighbors  = 0,
BFD Status                 = Disabled,
DR-Only Option for BFD     = Disabled
```

Output fields when an interface name is specified are described below:

output definitions

Interface IP Name	The name of the VLAN to which the interface is assigned.
VLAN Id	The VLAN to which the interface is assigned.
Interface IP Address	The IP address assigned to the interface.
Interface IP Mask	The IP mask associated with the IP address assigned to the interface.
Admin Status	The current administration status of the interface, either enabled or disabled .
Operational Status	Whether the interface is an active OSPF interface.
OSPF Interface State	The current state of the OSPF interface. It will be down , up , dp , dr , or other .
Interface Type	The OSPF interface type, which can be Broadcast, NBMA, Point-to-Point, or Point-to-Multipoint.
Area Id	The area identification number to which the interface is assigned. This field is not applicable if an interface has not yet been assigned to an area.
Designated Router IP Address	The designated router IP address.

output definitions (continued)

Designated Router RouterId	The identification number of the designated router.
Backup Designated Router IP Address	The IP address of the backup designated router.
Backup Designated Router RouterId	The identification number of the backup designated router.
MTU	The Maximum Transfer Unit (in bytes) for the interface.
Metric Cost	The cost added to routes learned on this interface.
Priority	The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.
Hello Interval	The number of seconds between hello messages sent out on the interface.
Transit Delay	The estimated number of seconds required to transmit a link state update over this interface.
Retrans Interval	The number of seconds the interface waits before resending hello messages.
Dead Interval	The number of seconds the interface waits for hello messages received from a neighbor before declaring the neighbor as dead.
Poll Interval	The larger time interval, in seconds, between hello messages sent to inactive neighbors.
Link Type	The IP interface type, either broadcast or non broadcast .
Authentication Type	The type of authentication used by this interface, either none , simple , or md5 .
#	The indexing of the MD5 key. (This field is only displayed for MD5 authentication.)
Id	A key identifier that identifies the algorithm and MD5 secret key associated with this interface. (This field is only displayed for MD5 authentication.)
Key	Indicates whether the MD5 key has been set or not. (This field is only displayed for MD5 authentication.)
Status	The status of the configured MD5 authentication key. (This field is only displayed for MD5 authentication.)
StartAccept	The time that the OSPF router will start accepting packets that have been created with this key. (This field is only displayed for MD5 authentication.)
StopAccept	The time that the OSPF router will stop accepting packets that have been created with this key. (This field is only displayed for MD5 authentication.)
StartGen	The time that the OSPF router will start using this key for packet generation. (This field is only displayed for MD5 authentication.)
StopGen	The time that the OSPF router will stop using this key for packet generation. (This field is only displayed for MD5 authentication.)
Authentication Key	This field displays whether the authentication key has been configured or not. (This field is only displayed for simple and no authentication.)
# of Events	The number of interface state machine events.

output definitions (continued)

# of Init State Neighbors	The number of OSPF neighbors in the initialization state.
# of 2-Way State Neighbors	The number of OSPF 2-way state neighbors on this interface.
# of Exchange State Neighbors	The number of OSPF neighbors in the exchange state.
# of Full State Neighbors	The number of OSPF neighbors in the full state. The full state is a neighbor that is recognized and passing data between itself and the interface.
BFD Status	The status of BFD on this interface.
DR-Only Option for BFD	The BFD setting for this interface. If DR-Only only is disabled then the setting is All Neighbors.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip ospf interface	Creates and deletes an OSPF interface.
ip ospf interface auth-key	Configures an OSPF authentication key for simple authentication on an interface.
ip ospf interface dead-interval	Configures the OSPF interface dead interval.
ip ospf interface hello-interval	Configures the OSPF interface hello interval.
ip ospf interface md5	Creates and deletes the OSPF interface MD5 key identification number.
ip ospf interface md5 key	Configures the OSPF key string.
ip ospf interface cost	Configures the OSPF interface cost.
ip ospf interface poll-interval	Configures the OSPF poll interval for a Non Broadcast Multi Access (NBMA) interface.
ip ospf interface priority	Configures the OSPF interface priority.
ip ospf interface retrans-interval	Configures the OSPF interface retransmit interval.
ip ospf interface transit-delay	Configures the OSPF interface transit delay.
ip ospf interface auth-type	Sets the OSPF interface authentication type.
ip ospf interface area	Configures an OSPF interface area.
ip ospf interface type	Configures the OSPF interface type.
ip ospf interface admin-state	Enables or disables the administration status on an OSPF interface.

MIB Objects

ospfIfTable

- ospfIfIpAddress
- ospfIfAreaId
- ospfIfType
- ospfIfAdminStat
- ospfIfRtrPriority
- ospfIfTransitDelay
- ospfIfRetransInterval
- ospfIfHelloInterval
- ospfIfRtrDeadInterval
- ospfIfPollInterval
- ospfIfState
- ospfIfDesignatedRouter
- ospfIfBackupDesignatedRouter
- ospfIfEvents
- ospfIfAuthType
- ospfIfStatus
- ospfIfAuthKey

alaOspfIfMd5Table

- alaOspfIfMd5IpAddress
- alaOspfIfMd5KeyId
- alaOspfIfMd5Key
- alaOspfIfMd5EncryptKey
- alaOspfIfMd5KeyStartAccept
- alaOspfIfMd5KeyStopAccept
- alaOspfIfMd5KeyStartGenerate
- alaOspfIfMd5KeyStopGenerate

alaOspfIfAugTable

- alaOspfIfIntfName

show ip ospf restart

Displays the OSPF graceful restart related configuration and status.

show ip ospf restart

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on OmniSwitch 10K switches with a single CMM.

Examples

```
-> show ip ospf restart
Restart Support                = Enabled,
Restart Interval (in seconds) = 120,
Restart Status                 = Not Restarting,
Restart Age (in seconds)      = 0,
Last Restart Exit Reason      = None,
Restart Helper Support        = Enabled,
Restart Helper Strict Checking = Enabled,
Restart Helper Mode           = NotHelping
```

output definitions

Restart Support	The administrative status of OSPF graceful restart, which can be Enabled or Disabled .
Restart Interval	The configured OSPF hitless restart timeout interval, in seconds. Use the ip ospf restart-interval command to modify this parameter.
Restart Status	The current status of OSPF graceful restart, which can be Not Restarting , Unplanned Restart (after a CMM takeover), or Planned Restart (before CMM takeover).
Restart Age	The remaining time, in seconds, for the current OSPF graceful restart interval.
Last Restart Exit Reason	The outcome of the last attempt at a graceful restart. If the value is None , then no restart has yet been attempted. If the value is In Progress , then a restart attempt is currently underway. Other possible values include Completed (successfully completed), Timed Out (timed out), and Topology Changed (aborted due to topology change).

output definitions (continued)

Restart Helper Support	The administrative status of the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart, which can be Enabled or Disabled . Use the ip ospf restart-helper admin-state command to modify this parameter.
Restart Helper Strict Checking	The administrative status of whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router, which can be Enabled or Disabled . Use the ip ospf restart-helper strict-lsa-checking admin-state command to modify this parameter.
Restart Helper Mode	Whether this OSPF router is operating as a helper to a restarting router.

21 OSPFv3 Commands

Open Shortest Path First version 3 (OSPFv3) routing is a shortest path first (SPF) or link-state protocol. This protocol is compatible with 128-bit IPv6 address space, while OSPF is compatible with 32-bit IPv4 address space. OSPFv3 is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPFv3 chooses the least-cost path as the best path.

Each participating router distributes its local state (i.e., the router's usable interfaces and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. This database is built from the collected link state advertisements of all routers. Each multi-access network that has at least two attached routers has a designated router and a backup designated router. The designated router floods a link state advertisement for the multi-access network and has other special responsibilities.

OSPFv3 allows collections of contiguous networks and hosts to be grouped together. A group, together with the routers having interfaces to any one of the included networks, is called an *area*. Each area runs a separate copy of the basic link-state routing algorithm. This means that each area has its own topological database, as explained in the previous section.

Alcatel-Lucent's version of OSPFv3 complies with RFCs 2740, 1826, 1827, 2553, 2373, 2374, and 2460.

MIB information for OSPFv3 is as follows:

Filename: AlcatelIND1DrcTm.mib
Module: ALCATEL-IND1-DRCTM-MIB

Filename: AlcatelIND1Ospf3.mib
Module: ALCATEL-IND1-OSPF3-MIB

Filename: IETF-OSPF-OSPFv3.MIB
Module: OSPF-OSPFv3-MIB

The following is a list of the commands for configuring OSPFv3:

Global OSPFv3 Commands	<code>ipv6 ospf admin-state</code> <code>ipv6 load ospf</code> <code>ipv6 ospf host</code> <code>ipv6 ospf mtu-checking</code> <code>ipv6 ospf route-tag</code> <code>ipv6 ospf spf-timer</code> <code>ipv6 ospf virtual-link</code> <code>show ipv6 ospf</code> <code>show ipv6 ospf border-routers</code> <code>show ipv6 ospf host</code> <code>show ipv6 ospf lsdb</code> <code>show ipv6 ospf neighbor</code> <code>show ipv6 ospf routes</code> <code>show ipv6 ospf virtual-link</code>
OSPFv3 Area Commands	<code>ipv6 ospf area</code> <code>show ipv6 ospf area</code>
OSPFv3 Interface Commands	<code>ipv6 ospf interface</code> <code>ipv6 ospf interface admin-state</code> <code>ipv6 ospf interface area</code> <code>ipv6 ospf interface dead-interval</code> <code>ipv6 ospf interface hello-interval</code> <code>ipv6 ospf interface cost</code> <code>ipv6 ospf interface priority</code> <code>ipv6 ospf interface retrans-interval</code> <code>ipv6 ospf interface transit-delay</code> <code>show ipv6 ospf interface</code>

ipv6 ospf admin-state

Enables or disables the OSPFv3 administrative status for the router.

ipv6 ospf admin-state {enable | disable}

Syntax Definitions

enable	Enables OSPFv3.
disable	Disables OSPFv3.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The OSPFv3 protocol should be enabled to route traffic.

Examples

```
-> ipv6 ospf admin-state enable
-> ipv6 ospf admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf Displays OSPFv3 status and general configuration parameters.

MIB Objects

```
ospfv3GeneralGroup
  ospfv3AdminStat
```

ipv6 load ospf

Loads the OSPFv3 software on the router.

ipv6 load ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Example

```
-> ipv6 load ospf
```

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

ALADRCTMCONFIG

alaDrcTmIPOspf3Status

ipv6 ospf host

Creates or deletes an OSPFv3 entry for directly attached hosts.

```
ipv6 ospf host ipv6_address [area area_id] [metric metric]
```

```
no ipv6 ospf host ipv6_address area area_id
```

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IP address of the OSPF host.
<i>area_id</i>	Area to which the host route belongs.
<i>metric</i>	The cost metric value assigned to the specified host. The valid range is 0–65535.

Defaults

parameter	default
<i>metric</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove the record of the OSPFv3 host.
- Use this command when multiple paths exist to a host. The specified host must be directly attached to the router. A metric value is the cost of all the hops necessary for a packet to reach its destination. Routers use the metric to determine the best possible path.
- This command allows you to modify the host parameter **metric**.

Examples

```
-> ipv6 ospf host 2001::1/64 metric 10  
-> no ipv6 ospf host 2001::1/64 metric 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf host](#) Displays information on the configured OSPFv3 hosts.

MIB Objects

ospfv3HostTable

- ospfv3HostStatus
- ospfv3HostAreaID
- ospfv3HostAddress
- ospfv3HostMetric

ipv6 ospf mtu-checking

Enables or disables Maximum Transfer Unit (MTU) checking. The MTU limits the size of a transmitted or received packet.

ipv6 ospf mtu-checking

no ipv6 ospf mtu-checking

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to disable MTU checking.
- This command is used to disable the checking for mismatch of the interface MTU while establishing a neighbor adjacency with a router. MTU mismatch occurs when a router receives packets that contain a larger MTU value than that of the interface on which adjacency is being established. The interface MTU is the largest IP datagram size (in bytes) that the interface can accept.

Examples

```
-> ipv6 ospf mtu-checking  
-> no ipv6 ospf mtu-checking
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf](#)

Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3  
  alaOspf3MTUCheck
```

ipv6 ospf route-tag

Configures a tag value for the Autonomous System External (ASE) routes created.

ipv6 ospf route-tag *tag*

Syntax Definitions

tag The set tag value. The valid range is 0–2, 147, 483, 647.

Defaults

parameter	default
<i>tag</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows you to set a tag value for ASE routes that are learned by this OSPF router. The tag value allows for quick identification.
- OSPF ASE route advertisements contain a tag value field. This field allows the exchange of information between autonomous system border routers (ASBRs).

Examples

```
-> ipv6 ospf route-tag 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf](#) Displays OSPFv3 status and general configuration parameters.

MIB Objects

alaProtocolOspf3
alaOspf3RedistRouteTag

ipv6 ospf spf-timer

Configures timers for Shortest Path First (SPF) calculation.

```
ipv6 ospf spf-timer [delay delay_seconds] [hold hold_seconds]
```

Syntax Definitions

delay_seconds Specifies time (from 0 to 65535 seconds) between the reception of an OSPF topology change and the start of an SPF calculation.

hold_seconds Specifies the minimum time (from 0 to 65535 seconds) between consecutive SPF calculations.

Defaults

parameter	default
<i>delay_seconds</i>	5
<i>hold_seconds</i>	10

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows you to configure the time interval between SPF calculations.
- Use the delay timer to determine how much time to postpone an SPF calculation after the router receives a topology change.
- Use the hold timer to configure the amount of time that must elapse between consecutive SPF calculations.
- There will be no delay in the SPF calculation if either the delay timer or hold timer is set to 0. The SPF calculations will occur immediately upon the reception of a topology change and/or that back-to back SPF calculations can take place with no break in-between the two.

Examples

```
-> ipv6 ospf spf-timer delay 20 hold 35
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf

Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
alaProtocolOspf3  
  alaOspf3TimerSpfDelay  
  alaOspf3TimerSpfHold
```

ipv6 ospf virtual-link

Creates or deletes a virtual link. A virtual link restores the backbone connectivity if the backbone is not physically contiguous.

```
ipv6 ospf virtual-link area area_id router router_id
[dead-interval seconds] [hello-interval seconds] [retrans-interval seconds] [transit-delay seconds]
```

```
no ipv6 ospf virtual-link area area_id router router_id
```

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
<i>router_id</i>	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
dead-interval <i>seconds</i>	Sets the virtual link dead interval. If no hello packets on this link for the set number of seconds have been received, the virtual neighbor is declared dead. The valid range is 1–2147483647.
hello-interval <i>seconds</i>	Sets the virtual link hello interval, which is the time interval between OSPF hellos sent on this virtual link. The valid range is 1–65535.
retrans-interval <i>seconds</i>	Sets the virtual link retransmit interval. The router waits the set number of seconds before retransmitting OSPF packets. The valid range is 0–3600.
transit-delay <i>seconds</i>	Sets the virtual link transit delay, which is the number of seconds to transmit OSPF packets over this link. The valid range is 0–3600.

Defaults

parameter	default
dead-interval <i>seconds</i>	40
hello-interval <i>seconds</i>	10
retrans-interval <i>seconds</i>	5
transit-delay <i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to delete the virtual link.
- You can define areas in such a way that the backbone is no longer contiguous. In this case, the system administrator can ensure backbone connectivity physically.
- Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.
- If authentication is enabled, both routers at either end of the virtual link must share the same password. Simple authentication refers to the use of only clear-text passwords as an authentication method. MD5 authentication refers to the usage of message digests.
- The **dead-interval** value should be the same for all the routers on the same network. This value should be a multiple of the value provided for the **hello-interval**.

Examples

```
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 dead-interval 50
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 hello-interval 20
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 retrans-interval 20
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 transit-delay 50
-> no ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf virtual-link](#) Displays the virtual link information.

MIB Objects

```
ospfv3VirtIfTable
  ospfv3VirtIfAreaId
  ospfv3VirtIfNeighbor
  ospfv3VirtIfStatus
  ospfv3VirtIfRtrDeadInterval
  ospfv3VirtIfHelloInterval
  ospfv3VirtIfRetransInterval
  ospfv3VirtIfTransitDelay
```

ipv6 ospf area

Assigns an OSPFv3 interface to a specified area.

ipv6 ospf area *area_id* [**type** {**normal** | **stub** [**default-metric** *metric*]}]

no ipv6 ospf area *area_id*

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IPv4 address format.
normal	Sets the area as a regular OSPFv3 area.
stub	Configures an OSPFv3 area as a stub area.
<i>metric</i>	Defines the metric to be used for default routes injected into the stub.

Defaults

parameter	default
normal stub	normal

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to delete the OSPFv3 area.
- The **default-metric** parameter defines the metric to be used for default routes injected into the stub area.

Examples

```
-> ipv6 ospf area 0.0.0.1
-> ipv6 ospf area 0.0.0.1 stub
-> ipv6 ospf area 0.0.0.1 type normal
-> no ipv6 ospf area 0.0.0.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf area](#) Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

MIB Objects

ospfv3AreaTable

ospfv3ImportAsExtern

ospfv3AreaSummary

ospfv3StubMetric

ospfv3AreaId

ipv6 ospf interface

Creates or deletes an OSPFv3 interface.

ipv6 ospf interface *interface_name*

no ipv6 ospf interface *interface_name*

Syntax Definitions

interface_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to delete an OSPFv3 interface.
- The interface name cannot contain spaces.

Examples

```
-> ipv6 ospf interface vlan-101  
-> no ipv6 ospf interface vlan-101
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface Displays the status and statistics of an OSPFv3 interface.

MIB Objects

ospfv3IfTable
ospfv3IfIndex

ipv6 ospf interface admin-state

Enables or disables the administration status on an OSPFv3 interface.

ipv6 ospf interface *interface_name* **admin-state** {enable | disable}

no ipv6 ospf interface *interface_name*

Syntax Definitions

<i>interface_name</i>	The name of the interface.
enable	Enables the OSPFv3 interface.
disable	Disables the OSPFv3 interface.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to delete an OSPFv3 interface.
- The OSPFv3 interface must be enabled to participate in the OSPFv3 protocol.

Examples

```
-> ipv6 ospf interface vlan-101 admin-state enable
-> ipv6 ospf interface vlan-101 admin-state disable
-> no ipv6 ospf interface vlan-101
-> no ipv6 ospf interface vlan-101
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable
  ospfv3IfIndex
  ospfv3IfAdminStat
```

ipv6 ospf interface area

Configures an OSPFv3 area identifier for this interface.

```
ipv6 ospf interface interface_name area area_id
```

Syntax Definitions

<i>interface_name</i>	The name of the interface.
<i>area_id</i>	A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

An interface must be assigned to an area to become operational.

Examples

```
-> ipv6 ospf interface vlan-101 area 0.0.0.1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf area	Displays either all the OSPFv3 areas, or a specified OSPFv3 area.
show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable  
  ospfv3IfIndex  
  ospfv3IfAreaId
```

ipv6 ospf interface dead-interval

Configures the OSPFv3 interface dead interval.

ipv6 ospf interface *interface_name* **dead-interval** *seconds*

Syntax Definitions

interface_name The name of the interface.

seconds The dead interval, in seconds. The valid range is 1–65535.

Defaults

parameter	default
<i>seconds</i> (broadcast and point-to-point)	40
<i>seconds</i> (NBMA and point-to-multi-point)	120

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- After the dead interval, a neighbor on this interface is considered dead if no hello packets have been received from this neighbor.
- This interval should be greater than the hello interval or multiples of the hello interval.

Examples

```
-> ipv6 ospf interface vlan-101 dead-interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 ospf interface hello-interval](#)

Configures the OSPFv3 interface hello interval.

[show ipv6 ospf interface](#)

Displays the status and statistics of an OSPFv3 interface.

MIB Objects

ospfv3IfTable

ospfv3IfIndex

ospfv3IfRtrDeadInterval

ipv6 ospf interface hello-interval

Configures the OSPFv3 interface hello interval.

```
ipv6 ospf interface interface_name hello-interval seconds
```

Syntax Definitions

<i>interface_name</i>	The name of the interface.
<i>seconds</i>	The hello interval, in seconds. The valid range is 0–65535. A value of 0 creates a passive OSPF interface.

Defaults

parameter	default
<i>seconds</i> (broadcast and point-to-point)	10
<i>seconds</i> (NBMA and point-to-multi-point)	30

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This is the interval between two consecutive hello packets sent out on this interface.

Examples

```
-> ipv6 ospf interface vlan-101 hello-interval 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf interface dead-interval	Configures the OSPFv3 interface dead interval.
show ipv6 ospf interface	Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable  
  ospfv3IfIndex  
  ospfv3IfHelloInterval
```

ipv6 ospf interface cost

Configures the OSPFv3 interface cost.

```
ipv6 ospf interface interface_name cost cost
```

Syntax Definitions

interface_name The name of the interface.

cost The interface cost. The valid range is 0–65535.

Defaults

parameter	default
<i>cost</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The configured interface cost (if any) is used during OSPFv3 route calculations.

Examples

```
-> ipv6 ospf interface vlan-101 cost 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf interface](#) Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable  
  ospfv3IfIndex  
  ospfv3IfMetricValue
```

ipv6 ospf interface priority

Configures the OSPFv3 interface priority. The priority number helps determine the eligibility of this router to become the designated router on the network.

ip ospf interface *interface_name* **priority** *priority*

Syntax Definitions

interface_name The name of the interface.

priority The interface priority. The valid range is 0–255.

Defaults

parameter	default
<i>priority</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the highest priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become the designated router.

Examples

```
-> ipv6 ospf interface vlan-101 priority 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf interface](#) Displays the status and statistics of an OSPFv3 interface.

MIB Objects

ospfv3IfTable
 ospfv3IfIndex
 ospfv3IfRtrPriority

ipv6 ospf interface retrans-interval

Configures the OSPFv3 interface retransmit time interval.

```
ipv6 ospf interface interface_name retrans-interval interval
```

Syntax Definitions

interface_name The name of the interface.

interval The retransmit interval, in seconds. The valid range 0–3600.

Defaults

parameter	default
<i>interval</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The number of seconds between link retransmission of OSPFv3 packets on this interface.

Examples

```
-> ipv6 ospf interface vlan-101 retrans-interval 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf interface](#) Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable  
  ospfv3IfIndex  
  ospfv3IfRetransInterval
```

ipv6 ospf interface transit-delay

Configures the OSPFv3 interface transit time delay.

```
ipv6 ospf interface interface_name transit-delay delay
```

Syntax Definitions

interface_name The name of the interface.

delay The transit delay, in seconds. The valid range is 0–3600.

Defaults

parameter	default
<i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The estimated number of seconds required to transmit a link state update over this interface. This command takes into account transmission and propagation delays and must be greater than 0.

Examples

```
-> ipv6 ospf interface vlan-101 transit-delay 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 ospf interface](#) Displays the status and statistics of an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable  
  ospfv3IfIndex  
  ospfv3IfTransitDelay
```

show ipv6 ospf

Displays the OSPFv3 status and general configuration parameters.

show ipv6 ospf

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display the general configuration parameters of the OSPFv3 router.
- See the Related Commands section below to modify the displayed parameters.

Examples

```
-> show ipv6 ospf
```

```
Status = Enabled,
Router ID = 5.5.5.5,
# Areas = 2,
# Interfaces = 4,
Area Border Router = Yes,
AS Border Router = No,
External Route Tag = 0,
SPF Hold (seconds) = 10,
SPF Delay (seconds) = 5,
MTU checking = Enabled,
# SPF calculations performed = 3,
Last SPF run (seconds ago) = N/A,
# of neighbors that are in:
  Full state = 3,
  Loading state = 0,
  Exchange state = 0,
  Exstart state = 0,
  2way state = 0,
  Init state = 0,
  Attempt state = 0,
  Down state = 0,
```

output definitions

Status	Displays whether OSPFv3 is currently enabled or disabled on the router.
Router Id	The unique identification for the router.
# Areas	Number of areas to which the router belongs.
# Interface	Number of interfaces participating in OSPF
Area Border Router	Displays whether the router status is an area router or not.
AS Border Router	Displays whether the area Autonomous System Border Router status of this router is enabled or disabled.
External Route Tag	Displays the route tag for this router.
SPF Hold (seconds)	Displays the time in seconds between the reception of an OSPFv3 topology change and the start of a SPF calculation.
SPF Delay (seconds)	Displays the time in seconds between consecutive SPF calculations.
MTU Checking	Displays whether Maximum Transfer Unit checking is enabled or disabled. This is set using the ipv6 ospf mtu-checking command.
# SPF calculations performed	Displays the number of SPF calculation performed.
Last SPF run (seconds ago)	N/A
Full state	Displays the number of neighbor routers that are in Full state.
Loading state	Displays the number of neighbor routers that are in Loading state.
Exchange state	Displays the number of neighbor routers that are in Exchange state.
Exstart state	Displays the number of neighbor routers that are in Exstart state.
2way state	Displays the number of neighbor routers that are in 2way state.
Init state	Displays the number of neighbor routers that are in Init state.
Attempt state	Displays the number of neighbor routers that are in Attempt state.
Down state	Displays the number of neighbor routers that are in Down state.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf admin-state	Enables or disables the administration of OSPFv3 on the router.
ipv6 ospf mtu-checking	Enables or disables the use of Maximum Transfer Unit (MTU) checking.
ipv6 ospf spf-timer	Configures timers for SPF calculation.
ipv6 ospf route-tag	Configures a tag value for Autonomous System External (ASE) routes created.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
ospfv3GeneralGroup
  ospfv3RouterId
  ospfv3AdminStat
  ospfv3VersionNumber
  ospfv3AreaBdrRtrStatus
  ospfv3ASBdrRtrStatus
  ospfv3OriginateNewLsas
  ospfv3RxNewLsas
  ospfv3ExitOverflowInterval
alaProtocolOspf3
  alaOspf3RedistAdminStatus
  alaOspf3RedistRouteTag
  alaOspf3TimerSpfDelay
  alaOspf3TimerSpfHold
  alaOspf3MTUCheck
```

show ipv6 ospf border-routers

Displays information regarding all or specified border routers.

show ipv6 ospf border-routers [**area** *area_id*] [**router** *router_id*]

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
<i>router_id</i>	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display a list of border routers known by this OSPFv3 router.
- By using the optional parameters, you can display the border routers using the specified parameter. For example, to find a router using a router ID of 1.1.1.1, enter the command using the router ID of 1.1.1.1 as a search criteria.
- See the Related Commands sections below to modify the list.

Examples

```
-> show ipv6 ospf border-routers
```

```
Router ID          Area          Metric  Type
-----+-----+-----+-----
6.6.6.6           0.0.0.0       2       INTRA
6.6.6.6           0.0.0.1       2       INTRA
    fe80::2d0:95ff:fee2:6bda -> pseudo1
    fe80::2d0:95ff:fee2:6bda -> pseudo2
```

output definitions

Router ID	The unique identification for the router.
Area	A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
Metric	The metric used by the routes.
Type	The type of routes specified (intra or inter).

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

N/A

show ipv6 ospf host

Displays information on the configured OSPFv3 hosts.

show ipv6 ospf host [*ipv6_address*]

Syntax Definitions

ipv6_address A 128-bit IP address for a directly attached host.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display general information for OSPFv3 hosts directly attached to this router.
- See the Related Commands section below to modify the list.

Examples

-> show ipv6 ospf host

```
Area           Metric   Address
-----+-----+-----
0.0.0.1        1       2001::1/64
```

output definitions

Area	A 32-bit IP address for a directly attached host. This can be set using the ipv6 ospf host command.
Metric	The metric assigned to the host. Metric is set using the ipv6 ospf host command.
Address	IPV6 address of the host.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 ospf host](#)

Creates or deletes an OSPFv3 entry for directly attached hosts.

MIB Objects

```
ospfv3HostTable  
  ospfv3HostIpAddress  
  ospfv3HostMetric  
  ospfHostStatus  
  ospfv3HostAreaID
```

show ipv6 ospf lsdb

Displays Link State Advertisements (LSAs) in the Link State Database (LSDB) associated with each area.

```
show ipv6 ospf lsdb [area area_id] [rtr | net | netsum | asbrsum] [linkstate-id ls_id] [router-id router_id]
```

Syntax Definitions

<i>area_id</i>	A unique 32-bit value in IP address format.
rtr	Specifies router LSAs.
net	Specifies network LSAs.
netsum	Specifies network summary LSAs.
asbrsum	Specifies Autonomous System Border Router summary LSAs.
<i>ls_id</i>	The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.
<i>router_id</i>	The Router ID. The ID is a unique 32-bit value such as an IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display the LSDB of the OSPF router. It can be used for OSPF debugging, specifically to narrow down sections of an area to determine which sections are receiving the specified LSAs. You can specify the parameters of only the area LSDB using the optional command parameters.
- You can view LSAs by specifying either a link state identifier or a router identifier. However, when specifying a router ID, you also need to supply a valid link state ID.

Examples

```
-> show ipv6 ospf lsdb
```

Area	Type	Link ID	Advertising Rtr	Sequence #	Age
0.0.0.0	Router	0	1.1.1.1	8000020f	1117
0.0.0.0	Router	0	3.3.3.3	80000208	1121
0.0.0.0	Router	0	5.5.5.5	800001f1	1117
0.0.0.0	Router	0	30.30.30.30	800000da	1115

output definitions

Area	The identification of the area to which the router belongs.
Type	The protocol type from where the route was learned.
Link ID	The Link state ID. The ID is a unique 32-bit value expressed as an IPv6 address. This number is used as a record in the link state database.
Advertising Rtr	The ID of the router that advertises the routes.
Sequence #	The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).
Age	The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 ospf admin-state](#) Displays the OSPFv3 status and general configuration parameters.

MIB Objects

```
ospfv3AsLsdbTable
  ospfv3AsLsdbAreaId
  ospfv3AsLsdbType
  ospfv3AsLsdbLsid
  ospfv3AsLsdbRouterId
  ospfv3AsLsdbAdvertisement
  ospfv3AsLsdbSequence
  ospfv3AsLsdbAge
```

show ipv6 ospf neighbor

Displays information on OSPFv3 non-virtual neighbors.

show ipv6 ospf neighbor [**router** *ipv4_address*][**interface** *interface_name*]

Syntax Definitions

ipv4_address A 32-bit router ID of the neighboring router.
interface_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to display all non-virtual neighbors of the OSPF router.
- See the Related Commands section below to modify the list.

Examples

```
-> show ipv6 ospf neighbor
```

Router ID	Area/Transit Area	State	Interface
1.1.1.1	0.0.0.0	FULL	vlan-2071
3.3.3.3	0.0.0.0	FULL	vlan-2071
5.5.5.5	0.0.0.0	FULL	vlan-2071
23.23.23.23	0.0.0.1	FULL	vlan-2055
23.23.23.23	0.0.0.1	FULL	vlan-2056
24.24.24.24	0.0.0.1	FULL	vlan-2065
24.24.24.24	0.0.0.1	FULL	vlan-2066

output definitions

Router ID	The unique identification for the router.
Area/Transit Area	The area identifier.
State	The state of the OSPF neighbor adjacency.
Interface	The name of the interface.

```
-> show ipv6 ospf neighbor router 24.24.24.24
```

Router ID	Area/Transit Area	State	Interface
24.24.24.24	0.0.0.1	FULL	vlan-2070
24.24.24.24	0.0.0.1	FULL	vlan-2073

output definitions

Router ID	The unique identification for the router.
Area/Transit Area	The area identifier.
State	The state of the OSPF neighbor adjacency.
Interface	The name of the interface.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
ospfv3NbrTable
  ospfNbrAddress
  ospfv3NbrRtrId
  ospfv3NbrOptions
  ospfv3NbrPriority
  ospfv3NbrState
  ospfv3NbrEvents
  ospfv3NbrHelloSuppressed
```

show ipv6 ospf routes

Displays the OSPFv3 routes known to the router.

show ipv6 ospf routes [**prefix** *ipv6_address_prefix*][**gateway** *gateway*]

Syntax Definitions

ipv6_address_prefix The 128-bit IPv6 address of the route destination in hexadecimal format.

gateway The next hop IPv6 address for this router.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If no variables are entered, all routes are displayed.
- If the variables are entered, then only routes matching the specified criteria are shown.
- All the variables described above must be entered for a route match. If all of the variables are not entered, an error message is returned.

Examples

```
-> show ipv6 ospf routes
```

Prefix	Path Type	Metric
		1 : 2
::/ 0	INTER	2 : -
fe80::2d0:95ff:fee0:710c -> vlan-2071		
2051::/64	INTRA	2 : -
fe80::2d0:95ff:feac:a59f -> vlan-2055		
fe80::2d0:95ff:feac:a59f -> vlan-2056		
fe80::2d0:95ff:fed7:747e -> vlan-2065		
fe80::2d0:95ff:fed7:747e -> vlan-2066		

output definitions

Prefix	The destination address of the IPv6 route in the hexadecimal format.
Path Type	The type of routes specified (intra or inter).
Metric	The cost of the route.

Release History

Release 7.1.1; command was introduced.

Related Commands**ipv6 ospf admin-state**

Displays the OSPFv3 status and general configuration parameters.

MIB ObjectsN/A

Related Commands**ipv6 ospf virtual-link**

Creates or deletes a virtual link.

MIB Objects

```
ospfv3VirtIfTable  
  ospfv3VirtIfAreaId  
  ospfv3VirtIfNeighbor  
  ospfv3VirtIfState
```

show ipv6 ospf area

Displays either all OSPFv3 areas, or a specified OSPFv3 area.

show ipv6 ospf area [*area_id*]

Syntax Definitions

area_id A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Allows you to view the details of a specified OSPFv3 area.
- If an OSPF area is not specified, all known areas for the OSPFv3 router will be displayed.
- See the Related Commands section below for information on modifying an area.

Examples

```
-> show ipv6 ospf area
```

Area ID	Type	Stub Metric	Number of Interfaces
0.0.0.0	Normal	NA	2
0.0.0.1	Normal	NA	2

```
-> show ipv6 ospf area 0.0.0.0
```

```
Area Type = Normal,
Area Stub Metric = 0,
# of SPF calculations = 52,
# Interfaces = 3,
# Router LSAs = 2,
# Network LSAs = 3,
# Intra-area-prefix LSAs = 4,
# Inter-area-prefix LSAs = 15,
# Inter-area-router LSAs = 0,
# hosts = 0,
```

output definitions

Area Type	The area type. This field will be normal or stub .
Area Stub Metric	Indicates whether the area is enabled or disabled.
# Router LSAs	The total number of Link State Advertisements for the Area.

output definitions (continued)

# Network LSAs	The total number of inter-area Link State Advertisements.
# of SPF calculations	The number of times the area has calculated the Shortest Path.
# Interfaces	The number of OSPF interfaces.
# Intra-area-prefix LSAs	The number of intra-area-prefix LSAs, which associates a list of IPv6 address prefixes with a router by referencing a router-LSA.
# Inter-area-prefix LSAs	The number of inter-area-prefix LSAs. Corresponds to Type 3 summary-LSA of OSPF.
# Inter-area-router LSAs	The number of inter-area-router LSAs. Corresponds to Type 4 summary-LSA of OSPF.
# hosts	The number of directly attached hosts.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf area	Creates or deletes an OSPFv3 area, assigning default metric, cost, and type.
show ipv6 ospf interface	Displays OSPFv3 interface information.

MIB Objects

```
ospfv3AreaTable
  ospfv3AreaId
  ospfv3ImportAsExtern
  ospfv3SpfRuns
  ospfv3AreaBdrRtrCount
  ospfv3AreaSummary
  ospfv3AreaStatus
```

show ipv6 ospf interface

Displays OSPFv3 interface information.

show ipv6 ospf interface [*interface_name*]

Syntax Definitions

interface_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Not specifying the interface name displays all known interfaces for the OSPFv3 router.

Examples

```
-> show ipv6 ospf interface
```

Name	DR Router ID	BDR Router ID	Admin Status	Oper Status	State
vlan-2071	5.5.5.5	0.0.0.0	Enabled	Up	DR
vlan-2055	7.7.7.7	5.5.5.5	Enabled	Up	BDR
vlan-2056	7.7.7.7	5.5.5.5	Enabled	Up	BDR

output definitions

Name	The name of the interface.
DR Router ID	The designated router address on this network segment. Make sure you configure a VLAN for the router IP. (See Chapter 4, “VLAN Management Commands,” for more information.)
BDR Router ID	The IP address of the backup designated router.
Vlan	The VLAN to which the interface is assigned.
Admin Status	The current administration status of the interface, either enabled or disabled .
Oper Status	Indicates whether the interface is an active OSPF interface.
State	The current state of the OSPF interface. It will be DR , BDR , other .

```

-> show ipv6 ospf interface vlan-2071
Type                               = BROADCAST,
Admin Status                        = Enabled,
IPv6 Interface Status              = Up,
Oper Status                         = Up,
State                               = DR,
Area                               = 0.0.0.0,
Priority                            = 100,
Cost                                = 1,
Designated Router                  = 3.3.3.3,
Backup Designated Router           = 0.0.0.0,
Hello Interval                     = 1,
Router Dead Interval               = 4,
Retransmit Interval                = 5,
Transit Delay                      = 1,
Ifindex                           = 17,
IPv6 'ifindex'                    = 2071,
MTU                                = 1500,
# of attached neighbors            = 0,
Globally reachable prefix #0       = 2071::2/64

```

Output fields when an IP address or interface name is specified are described below:

output definitions

Type	The OSPF interface type, which can be Broadcast, NBMA, Point-to-Point, or Point-to-Multipoint.
Admin Status	The current administrative status of the interface, either enabled or disabled .
IPv6 Interface Status	The current administrative status of the IPv6 interface, either up or down .
Oper Status	Indicates whether the interface is an active OSPF interface.
State	The current state of the OSPF interface. It will be down , up , dp , dr , or other .
Area	The area identification number to which the interface is assigned. This field is not applicable if an interface has not yet been assigned to an area.
Priority	The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.
Cost	The cost added to routes learned on this interface.
Designated Router	The identification number of the designated router.
Backup Designated Router	The identification number of the backup designated router.
Hello Interval	The number of seconds between hello messages sent out on the interface.
Router Dead Interval	The number of seconds the interface waits for hello messages received from a neighbor before declaring the neighbor as dead.
Retransmit Interval	The number of seconds the interface waits before resending hello messages.
Transit Delay	The estimated number of seconds required to transmit a link state update over this interface.

output definitions (continued)

Ifindex	The unique value assigned to an interface.
IPv6 'ifindex'	The unique value assigned to an IPv6 interface.
MTU	The Maximum Transfer Unit (in bytes) for the interface.
# of attached neighbors	The number of OSPFv3 neighbors in the initialization state.
Globally reachable prefix #0	A globally unique IPv6 address.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf interface	Creates and deletes an OSPFv3 interface.
ipv6 ospf interface dead-interval	Configures the OSPFv3 interface dead interval.
ipv6 ospf interface hello-interval	Configures the OSPFv3 interface hello interval.
ipv6 ospf interface cost	Configures the OSPFv3 interface cost.
ipv6 ospf interface priority	Configures the OSPFv3 interface priority.
ipv6 ospf interface retrans-interval	Configures the OSPFv3 interface retransmit interval.
ipv6 ospf interface transit-delay	Configures the OSPFv3 interface transit delay.
ipv6 ospf interface area	Configures an OSPFv3 interface area.
ipv6 ospf interface admin-state	Enables or disables the administration status on an OSPFv3 interface.

MIB Objects

```
ospfv3IfTable  
  ospfv3IfAreaId  
  ospfv3IfType  
  ospfv3IfAdminStat  
  ospfv3IfRtrPriority  
  ospfv3IfTransitDelay  
  ospfv3IfRetransInterval  
  ospfv3IfHelloInterval  
  ospfv3IfRtrDeadInterval  
  ospfv3IfPollInterval  
  ospfv3IfState  
  ospfv3IfDesignatedRouter  
  ospfv3IfBackupDesignatedRouter  
  ospfv3IfEvents  
  ospfv3IfStatus
```

22 BGP Commands

This chapter describes the CLI commands used to configure the BGP (Border Gateway Protocol) and Multiprotocol extensions to BGP. BGP is a protocol for exchanging routing information between gateway hosts in a network of ASs (autonomous systems). BGP is the most common protocol used between gateway hosts on the Internet. The routing table exchanged contains a list of known routers, the addresses they can reach, and a preference metrics associated with the path to each router so that the best available route is chosen.

Multiprotocol Extensions to BGP-4 supports the exchange of IPv6 unicast prefixes, as well as the establishment of BGP peering sessions with BGP speakers identified by their IPv6 addresses.

The Alcatel-Lucent implementation of BGP-4 and Multiprotocol Extensions to BGP-4 complies with the following RFCs: 4271, 2439, 3392, 2385, 1997, 4456, 3065, 4273, 4760, 2545

Note. In the following document, the BGP terms “peer” and “neighbor” are used interchangeably to mean any BGP speaker known to the local router.

MIB information for BGP is as follows:

Filename: AlcatelIND1Bgp.MIB
Module: ALCATEL-IND1-BGP-MIB

Filename: IETF_BGP4.MIB
Module: BGP4-MIB

The following table summarizes the available commands:

Global BGP Commands	<ul style="list-style-type: none"> ip load bgp ip bgp admin-state ip bgp autonomous-system ip bgp bestpath as-path ignore ip bgp cluster-id ip bgp default local-preference ip bgp fast-external-failover ip bgp always-compare-med ip bgp bestpath med missing-as-worst ip bgp client-to-client reflection ip bgp as-origin-interval ip bgp synchronization ip bgp confederation identifier ip bgp maximum-paths ip bgp log-neighbor-changes ip bgp dampening ip bgp dampening clear show ip bgp show ip bgp statistics show ip bgp dampening show ip bgp dampening-stats show ip bgp path show ip bgp routes
Aggregate Configuration	<ul style="list-style-type: none"> ip bgp aggregate-address ip bgp aggregate-address admin-state ip bgp aggregate-address as-set ip bgp aggregate-address community ip bgp aggregate-address local-preference ip bgp aggregate-address metric ip bgp aggregate-address summary-only show ip bgp aggregate-address
Network (local route) Configurations	<ul style="list-style-type: none"> ip bgp network ip bgp network admin-state ip bgp network community ip bgp network local-preference ip bgp network metric show ip bgp network

Neighbor (Peer) Configuration	ip bgp neighbor
	ip bgp neighbor admin-state
	ip bgp neighbor advertisement-interval
	ip bgp neighbor clear
	ip bgp neighbor route-reflector-client
	ip bgp neighbor default-originate
	ip bgp neighbor timers
	ip bgp neighbor conn-retry-interval
	ip bgp neighbor auto-restart
	ip bgp neighbor maximum-prefix
	ip bgp neighbor md5 key
	ip bgp neighbor ebgp-multihop
	ip bgp neighbor description
	ip bgp neighbor next-hop-self
	ip bgp neighbor passive
	ip bgp neighbor remote-as
	ip bgp neighbor remove-private-as
	ip bgp neighbor soft-reconfiguration
	ip bgp neighbor stats-clear
	ip bgp confederation neighbor
	ip bgp neighbor update-source
	ip bgp neighbor in-aspathlist
	ip bgp neighbor in-communitylist
	ip bgp neighbor in-prefixlist
	ip bgp neighbor out-aspathlist
	ip bgp neighbor out-communitylist
	ip bgp neighbor out-prefixlist
	ip bgp neighbor route-map
	ip bgp neighbor clear soft
	show ip bgp neighbors
	show ip bgp neighbors policy
	show ip bgp neighbors timer
	show ip bgp neighbors statistics

Policy Commands	ip bgp policy aspath-list ip bgp policy aspath-list action ip bgp policy aspath-list priority ip bgp policy community-list ip bgp policy community-list action ip bgp policy community-list match-type ip bgp policy community-list priority ip bgp policy prefix-list ip bgp policy prefix-list action ip bgp policy prefix-list ge ip bgp policy prefix-list le ip bgp policy prefix6-list ip bgp policy route-map action ip bgp policy route-map aspath-list ip bgp policy route-map asprepend ip bgp policy route-map community ip bgp policy route-map community-list ip bgp policy route-map community-mode ip bgp policy route-map lpref ip bgp policy route-map lpref-mode ip bgp policy route-map match-community ip bgp policy route-map match-mask ip bgp policy route-map match-prefix ip bgp policy route-map match-regexp ip bgp policy route-map med ip bgp policy route-map med-mode ip bgp policy route-map origin ip bgp policy route-map prefix-list ip bgp policy route-map weight ip bgp policy route-map community-strip show ip bgp policy aspath-list show ip bgp policy community-list show ip bgp policy prefix-list show ip bgp policy route-map
BGP Graceful Restart Commands	ip bgp graceful-restart ip bgp graceful-restart restart-interval
IPv6 Global BGP Commands	ip bgp unicast ipv6 bgp unicast ip bgp neighbor activate-ipv6 ip bgp neighbor ipv6-next-hop show ipv6 bgp path show ipv6 bgp routes
IPv6 BGP Network Configuration Commands	ipv6 bgp network ipv6 bgp network community ipv6 bgp network local-preference ipv6 bgp network metric ipv6 bgp network admin-state show ipv6 bgp network

**IPv6 BGP Neighbor (Peer)
Configuration Commands**

`ipv6 bgp neighbor`
`ipv6 bgp neighbor activate-ipv6`
`ipv6 bgp neighbor ipv6-nexthop`
`ipv6 bgp neighbor admin-state`
`ipv6 bgp neighbor remote-as`
`ipv6 bgp neighbor timers`
`ipv6 bgp neighbor maximum-prefix`
`ipv6 bgp neighbor next-hop-self`
`ipv6 bgp neighbor conn-retry-interval`
`ipv6 bgp neighbor default-originate`
`ipv6 bgp neighbor update-source`
`ipv6 bgp neighbor ipv4-nexthop`
`show ipv6 bgp neighbors`
`show ipv6 bgp neighbors statistics`
`show ipv6 bgp neighbors policy`
`show ipv6 bgp neighbors policy`

ip load bgp

Loads the BGP protocol software into running memory on the router. The image file containing BGP should already be resident in flash memory before issuing this command.

ip load bgp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command requires that the BGP software be resident in flash memory in the active directory.
- Enter this command in the router's configuration file (boot.cfg) to ensure BGP software is running after a reboot.
- The command does not administratively enable BGP on the router; BGP will be disabled after issuing this command. You must issue the **ip bgp admin-state** to start the BGP protocol.

Examples

```
-> ip load bgp
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|---------------------------------|--|
| ip bgp autonomous-system | Configures the Autonomous system number for this BGP router. |
| ip bgp admin-state | Administratively enables or disables BGP. |

MIB Objects

alaDrcTmIPBgpStatus

ip bgp admin-state

Administratively enables or disables BGP. The BGP protocol will not be active until you enable it using this command.

ip bgp admin-state {enable | disable}

Syntax Definitions

enable	Enables BGP.
disable	Disables BGP.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You must first load the BGP software into running memory using the [ip load bgp](#) command before initiating this command.
- Many BGP commands require that the protocol be disabled ([ip bgp admin-state](#)) before issuing them.

Examples

```
-> ip bgp admin-state enable  
-> ip bgp admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip load bgp](#) Loads the BGP software.

MIB Objects

```
alaBgpGlobal  
  alaBgpProtoStatus
```

ip bgp autonomous-system

Configures the Autonomous System (AS) number for this router. This number identifies this BGP speaker (this router) instance to other BGP routers. The AS number for a BGP speaker determines whether it is an internal or an external peer in relation to other BGP speakers. BGP routers in the same AS are internal peers while BGP routers in different ASs are external peers. BGP routers in the same AS exchange different routing information with each other than they exchange with BGP routers in external ASs. BGP speakers append their AS number to routes passing through them; this sequence of AS numbers is known as a route's AS path.

ip bgp autonomous-system *value*

Syntax Definitions

value The AS number. The valid range is 1–65535.

Defaults

parameter	default
<i>value</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A router can belong to only one AS. Do not specify more than one AS value for each router.
- The BGP protocol must be disabled (using the [ip bgp admin-state](#) command) before using this command.

Examples

```
-> ip bgp autonomous-system 64724
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp admin-state](#) Enables and disables the BGP protocol.

MIB Objects

```
alaBgpGlobal
  alaBgpAutonomousSystemNumber
```

ip bgp bestpath as-path ignore

Indicates whether AS path comparison will be used in route selection. The AS path is the sequence of ASs through which a route has traveled. A shorter AS path is preferred over a longer AS path. The AS path is always advertised in BGP route updates. This command informs BGP to use the length of the AS path as a criteria for determining the best route.

ip bgp bestpath as-path ignore

no ip bgp bestpath as-path ignore

Syntax Definitions

N/A

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable this feature after it has been enabled.
- AS path comparison does not consider the type of links connecting the ASs along the path. In some cases a longer path over very fast connections may be a better route than a shorter path over slower connections. For this reason the AS path should not be the only criteria used for route selection. BGP considers local preference before AS path when making path selections.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp bestpath as-path ignore  
-> no ip bgp bestpath as-path ignore
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address as-set Specifies whether AS path aggregation is to be performed or not.

ip bgp policy aspath-list Creates or removes an AS path list.

ip bgp default local-preference Configures the default local preference (lpref) value to be used when advertising routes.

MIB Objects

alaBgpGlobal

alaBgpAsPathCompare

ip bgp cluster-id

Configures a BGP cluster ID when there are multiple, redundant, route reflectors in a cluster. This command is not necessary for configurations containing only one route reflector.

ip bgp cluster-id *ip_address*

Syntax Definitions

ip_address 32-bit IP address that is the Cluster ID of the router acting as a route reflector.

Defaults

parameter	default
<i>ip_address</i>	0.0.0.0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- In a route-reflection configuration where there are multiple route-reflectors in a cluster, use this command to configure this cluster ID. Configuring multiple route-reflectors enhances redundancy and avoids a single point of failure. When there is only one reflector in a cluster, the router ID of the reflector is used as the cluster-ID.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.
- Using many redundant reflectors in a single cluster places demands on the memory required to store routes for all redundant reflectors' peers.

Examples

```
-> ip bgp cluster-id 1.2.3.4
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp admin-state Enables and disables BGP.

ip bgp client-to-client reflection Enables route reflection and sets this speaker as the route reflector.

MIB Objects

alaBgpGlobal

alaBgpClusterId

ip bgp default local-preference

Configures the default local preference (lpref) value to be used when advertising routes. A higher local preference value is preferred over a lower value. The local preference value is sent to all BGP peers in the local autonomous system; it is not advertised to external peers.

ip bgp default local-preference *value*

Syntax Definitions

value The default local preference value for this router. The valid range is 0–4294967295.

Defaults

parameter	default
<i>value</i>	100

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- Unless a route is specifically configured for a different local preference value it will default to value you specify in this command. This value is used for routes learned from external autonomous systems (the local preference value is not advertised in routes received from external peers) and for aggregates and networks that do not already contain local preference values.
- This value is specific to the router so it can compare its own local preference to those received in advertised paths. If other routers belong to the same AS, then they should use the same default local preference value.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp default local-preference 200
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address local-preference Sets the local preference for a BGP aggregate.

ip bgp network local-preference Sets the local preference for a BGP network.

MIB Objects

alaBgpGlobal

alaBgpDefaultLocalPref

ip bgp fast-external-failover

Enables fast external failover (FEFO). When enabled, FEFO resets a session when a link to a directly connected external peer is operationally down. The BGP speaker will fall back to Idle and then wait for a connection retry by the external peer that went down.

ip bgp fast-external-failover

no ip bgp fast-external-failover

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable Fast External Failover.
- When enabled, this command allows BGP to take immediate action when a directly connected interface, on which an external BGP session is established, goes down. Normally BGP relies on TCP to manage peer connections. Fast External failover improves upon TCP by resetting connections as soon as they go down.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp fast-external-failover
-> no ip bgp fast-external-failover
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp neighbor clear](#)

Restarts a BGP peer.

[ip bgp neighbor auto-restart](#)

Enables or disables BGP peer automatic restart.

[ip bgp neighbor timers](#)

Configures the time interval between KEEPALIVE messages sent by this peer and the tolerated hold time interval, in seconds, for messages to this peer from other peers.

MIB Objects

alaBgpFastExternalFailOver

ip bgp always-compare-med

Enables or disables Multi-Exit Discriminator (MED) comparison between peers in different autonomous systems. The MED value is considered when selecting the best path among alternatives; it indicates the weight for a particular exit point from the AS. A path with a lower MED value is preferred over a path with a higher MED value.

ip bgp always-compare-med

no ip bgp always-compare-med

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable MED comparison for external peers.
- By default, BGP only compares MEDs from the same autonomous system when selecting routes. Enabling this command forces BGP to also compare MEDs values received from external peers, or other autonomous systems.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp always-compare-med
-> no ip bgp always-compare-med
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp bestpath med missing-as-worst Configures the MED parameter when it is missing in a BGP path.

MIB Objects

```
alaBgpGlobal
  alaBgpMedAlways
```

ip bgp bestpath med missing-as-worst

Configures the MED parameter when it is missing in a BGP path.

ip bgp bestpath med missing-as-worst

no ip bgp bestpath med missing-as-worst

Syntax Definitions

N/A

Defaults

By default this command is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable missing MEDs as worst.
- This command is used to specify how a missing MED in an external BGP path is to be treated for route selection purposes. The default behavior is to treat missing MEDs as zero (best). This command allows you to treat missing MEDs as worst ($2^{32}-1$) for compatibility reasons.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp bestpath med missing-as-worst  
-> no ip bgp bestpath med missing-as-worst
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp always-compare-med Forces BGP to consider MED values from external routes.

MIB Objects

alaBgpGlobal
alaBgpMissingMed

ip bgp client-to-client reflection

Enables or disables this BGP speaker (router) to be a route reflector. Route reflectors advertise routing information to internal BGP peers, referred to as *clients*. BGP requires all internal routers to know all routes in an AS. This requirement demands a fully meshed (each router has a direct connection to all other routers in the AS) topology. Route reflection loosens the fully meshed restriction by assigning certain BGP routers as route reflectors, which take on the responsibility of advertising routing information to local BGP peers.

ip bgp client-to-client reflection

no ip bgp client-to-client reflection

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable the speaker as a route reflector.
- In addition to defining this router as the route reflector, this command also enable route reflection for this cluster. After setting this command this reflector will begin using route reflection behavior when communicating to client and non-client peers.
- Once route reflectors are configured, you need to indicate the clients (those routers receiving routing updates from the reflectors) for each route reflector. Use the **ip bgp neighbor route-reflector-client** command to configure clients.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp client-to-client reflection
-> no ip bgp client-to-client reflection
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp admin-state Administratively disables BGP in this router.

ip bgp neighbor route-reflector-client Configures a BGP peer to be a client to the this route reflector.

MIB Objects

alaBgpGlobal

alaBgpRouteReflection

ip bgp as-origin-interval

Specifies the frequency at which routes local to the autonomous system are advertised. These advertisements are also referred to as UPDATE messages. This interval applies to advertisements to internal peers.

ip bgp as-origin-interval *seconds*

no ip bgp as-origin-interval

Syntax Definitions

seconds The update interval in seconds. The valid range is 1–65535.

Defaults

parameter	default
<i>seconds</i>	15

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to reset the feature to the default value.
- A lower value may increase the likelihood of route flapping as route status is updated more frequently.

Examples

```
-> ip bgp as-origin-interval 15
-> no ip bgp as-origin-interval
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp neighbor advertisement-interval](#) Set the route advertisement interval for external peers.

MIB Objects

```
alaBgpGlobal
  alaBgpAsOriginInterval
```

ip bgp synchronization

Enables or disables synchronization of BGP prefixes with AS-internal routing information. Enabling this command will force the BGP speaker to advertise prefixes only if the prefixes are reachable through AS-internal routing protocols (IGPs like RIP and OSPF).

ip bgp synchronization

no ip bgp synchronization

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable IGP synchronization.
- A BGP router is not supposed to advertise routes learned through internal BGP updates unless those routes are also known by the primary internal routing protocol (e.g, RIP or OSPF). However, requiring all routers in an AS to know all external routes places a heavy burden on routers focusing mainly on Intra-AS routing. Therefore, disabling synchronization avoids this extra burden on internal routers. As long as all BGP routers in an AS are fully meshed (each has a direct connection to all other BGP routers in the AS) then the problem of unknown external router should not be a problem and synchronization can be disabled.
- By default, synchronization is disabled and the BGP speaker can advertise a route without waiting for the IGP to learn it. When the autonomous system is providing transit service, BGP should not propagate IGP paths until the IGP prefixes themselves are known to be reachable through IGP. If BGP advertises such routes before the IGP routers have learned the path, they will drop the packets causing a blackhole.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp synchronization
-> no ip bgp synchronization
```

Release History

Release 7.1.1; command was introduced.

Related Commands**show ip bgp**

Displays the current global settings for the local BGP speaker.

MIB Objects

alaBgpGlobal

 alaBgpIgpSynchStatus

ip bgp confederation identifier

Sets a confederation identification value for the local BGP speaker (this router). A confederation is a grouping of sub-ASs into a single AS. To peers outside a confederation, the confederation appears to be a single AS. Within the confederation multiple ASs may exist and even exchange information with each other as using external BGP (EBGP).

ip bgp confederation identifier *value*

Syntax Definitions

value The confederation identification value. The valid range is 0–65535.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to restore the default value.
- A value of 0 means this local speaker is not a member of any confederation.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.
- Use this command in conjunction with the **ip bgp confederation neighbor** command to specify those peers that are a members of the same confederation as the local BGP speaker.

Examples

```
-> ip bgp confederation identifier 3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bgp autonomous-system** Sets the AS number for this router.
- ip bgp confederation neighbor** Specifies peers that are members of a confederation.

MIB Objects

alaBgpGlobal
alaBgpConfedId

ip bgp maximum-paths

Enables or disables support for multiple equal paths. When multipath support is enabled and the path selection process determines that multiple paths are equal when the router-id is disregarded, then all equal paths are installed in the hardware forwarding table. When multipath support is disabled, only the best route entry is installed in the hardware forwarding table.

ip bgp maximum-paths

no ip bgp maximum-paths

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable support for multiple equal cost paths.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

```
-> ip bgp maximum-paths
-> no ip bgp maximum-paths
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
  alaBgpMultiPath
```

ip bgp log-neighbor-changes

Enables or disables the logging of peer state changes. If enabled, this logging tracks changes in the state of BGP peers from ESTABLISHED to IDLE and from IDLE to ESTABLISHED. Viewing peer state logging requires that certain debug parameters be set.

ip bgp log-neighbor-changes

no ip bgp log-neighbor-changes

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The BGP protocol must be disabled (using the [ip bgp admin-state](#) command) before using this command.

Examples

```
-> ip bgp log-neighbor-changes
-> no ip bgp log-neighbor-changes
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp admin-state](#) Disables BGP within the router.

MIB Objects

```
alaBgpGlobal
  alaBgpPeerChanges
```

ip bgp dampening

Enables or disables BGP route dampening or the suppression of unstable routes. Route dampening helps to control the advertisement of routes that are going up and then down at an abnormally high rate. Routes that are changing states (available then unavailable) are said to be *flapping*.

ip bgp dampening [**half-life** *half_life* **reuse** *reuse* **suppress** *suppress* **max-suppress-time** *max_suppress_time*]

no ip bgp dampening

Syntax Definitions

<i>half_life</i>	The half-life duration, in seconds. The valid range is 0–65535.
<i>reuse</i>	The number of route withdrawals set for the re-use value. The valid range is 1–9999.
<i>suppress</i>	The dampening cutoff value. The valid range is 1–9999.
<i>max_suppress_time</i>	The maximum number of seconds a route can be suppressed. The valid range is 0–65535.

Defaults

parameter	value
<i>half_life</i>	300
<i>reuse</i>	200
<i>suppress</i>	300
<i>max_suppress_time</i>	1800

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable dampening.
- BGP dampening is disabled by default. When enabled, route dampening suppresses routes that are unstable, or “flapping,” and disrupting the network.
- BGP dampening of IPv6 route flaps is currently not supported.
- This command enables dampening and can also be used to change the default times for the dampening variables.
- Use the dampening variables to set penalties, suppression limits, and reuse values for flapping routes.

- The half-life value configures the half-life duration for a reachable route. After the time interval specified in this command, the penalty value for the route will be reduced by half. This command sets the duration in seconds during which the accumulated stability value is reduced by half if the route is considered reachable, whether suppressed or not. A larger value may be desirable for routes that are known for their instability. A larger value will also result in a longer suppression time if the route exceeds the flapping rate.
- The reuse value configures the number of route withdrawals necessary to begin readvertising a previously suppressed route. If the penalty value for a suppressed route fall below this value, then it will be advertised again. This command sets the reuse value, expressed as a number of route withdrawals. When the stability value for a route reaches or falls below this value, a previously suppressed route will be advertised again. The instability metric for a route is decreased by becoming more stable and by passing half-life time intervals.
- The suppress value configures the cutoff value, or number of route withdrawals, at which a flapping route is suppressed and no longer advertised to BGP peers. This value is expressed as a number of route withdrawals. When the stability value for a route exceeds this cutoff value, the route advertisement is suppressed.
- The max-suppress-time value configures the maximum time (in seconds) a route can be suppressed. This time is also known as the maximum holdtime or the maximum instability value. Once this time is reached the route flap history for a route will be deleted and the route will be advertised again (assuming it is still reachable). This maximum holdtime as applied on an individual route basis. Each suppressed route will be held for the amount of time specified in this command unless the route is re-advertised by falling below the reuse value.
- Entering the command with no variables returns the variables back to their defaults.

Examples

```
-> ip bgp dampening
-> ip bgp dampening half-life 20 reuse 800 suppress 60 max-suppress-time 40
-> no ip bgp dampening
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp dampening clear	Clears the dampening history data for all routes on the router, resetting route flap counters and unsuppressing any routes that had been suppressed due to route flapping violations.
show ip bgp dampening	Displays the BGP route dampening settings.
show ip bgp dampening-stats	Displays BGP dampening statistics.

MIB Objects

alaBgpGlobal

- alaBgpDampening
- alaBgpDampMaxFlapHistory
- alaBgpDampHalfLifeReach
- alaBgpDampReuse
- alaBgpDampCutOff

ip bgp dampening clear

Clears the dampening history data for all routes on the router, resetting route flap counters and unsuppressing any routes that had been suppressed due to route flapping violations.

ip bgp dampening clear

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to clear all of the currently stored information on routes for dampening purposes. When this command is entered, all route information in regards to dampening is cleared.
- BGP dampening of IPv6 route flaps is currently not supported.

Examples

```
-> ip bgp dampening clear
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp dampening](#) Enables or disables route dampening.

MIB Objects

```
alaBgpGlobal  
  alaBgpDampeningClear
```

ip bgp aggregate-address

Creates and deletes a BGP aggregate route. Aggregate routes are used to reduce the size of routing tables by combining the attributes of several different routes and allowing a single aggregate route to be advertised to peers.

The base command (**ip bgp aggregate-address**) may be used with other keywords to set up aggregate address configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

Note that only one of the following optional keywords is specified with each use of the base command. Keywords are not combined together in a single command.

ip bgp aggregate-address *ip_address ip_mask*

[**admin-state** {**enable** | **disable**}]

[**as-set**]

[**community** *string*]

[**local-preference** *value*]

[**metric** *metric*]

[**summary-only**]

no ip bgp aggregate-address *ip_address ip_mask*

Syntax Definitions

<i>ip_address</i>	32-bit IP address to be used as the aggregate address.
<i>ip_mask</i>	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete an aggregate route.
- This command allows administrative operations on a BGP aggregate. You must still enable the aggregate route through the **ip bgp aggregate-address admin-state** command.
- You cannot aggregate an address (for example, 100.10.0.0) if you do not have at least one more-specific route of the address (for example, 100.10.20.0) in the BGP routing table.
- Only the aggregate is advertised unless aggregate summarization is disabled using the **ip bgp aggregate-address summary-only** command.

Examples

```
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0  
-> no ip bgp aggregate-address 172.22.2.0 255.255.255.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp aggregate-address
summary-only](#)

Enables or disables aggregate summarization, which suppresses more-specific routes.

MIB Objects

```
alaBgpAggrAddr  
alaBgpAggrSet  
alaBgpAggrCommunity  
alaBgpAggrLocalPref  
alaBgpAggrMetric  
alaBgpAggrSummarize  
alaBgpAggrMask
```

ip bgp aggregate-address admin-state

Enables or disables a BGP aggregate route.

```
ip bgp aggregate-address ip_address ip_mask admin-state {enable | disable}
```

Syntax Definitions

<i>ip_address</i>	32-bit IP address for this aggregate route.
<i>ip_mask</i>	32-bit subnet mask that determines how many bits of the network address denote the network number.
enable	Enables this aggregate route.
disable	Disables this aggregate route.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Configure all aggregate route parameters before enabling the aggregate with this command. Use the [ip bgp aggregate-address](#) command to configure individual aggregate parameters.
- The [show ip bgp path](#) command displays every aggregate currently defined.

Examples

```
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0 admin-state enable  
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands**ip bgp aggregate-address**

Creates an aggregate route.

show ip bgp path

Displays aggregate routes.

MIB Objects

alaBgpAggrTable

alaBgpAggrAddr

 alaBgpAggrMask

ip bgp aggregate-address as-set

Specifies whether AS path aggregation is to be performed or not. AS path aggregation takes the AS path for all routes in this aggregate and creates a new AS path for the entire aggregate. This aggregated AS path includes all the ASs from the routes in the aggregate, but it does not repeat AS numbers if some routes in the aggregate include the same AS in their path.

ip bgp aggregate-address *ip_address ip_mask as-set*

no ip bgp aggregate-address *ip_address ip_mask as-set*

Syntax Definitions

ip_address 32-bit IP address.

ip_mask 32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable the **as-set** option.
- When AS path aggregation is disabled (the default), the AS path for the aggregate defaults to the AS number of the local BGP speaker (configured in the **ip bgp autonomous-system** command).
- If AS path aggregation is enabled, a flap in a more specific path's AS path will cause a flap in the aggregate as well.
- Do not use this command when aggregating many paths because of the numerous withdrawals and updates that must occur as path reachability information for the summarized routes changes.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 as-set
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 as-set
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address Creates and deletes a BGP aggregate route.

MIB Objects

alaBgpAggrTable
 alaBgpAggrAddr
 alaBgpAggrMask
 alaBgpAggrSet

ip bgp aggregate-address community

Defines a community for an aggregate route created by the **ip bgp aggregate-address** command. Communities are a way of grouping BGP peers that do not share an IP subnet or an AS number.

ip bgp aggregate-address *ip_address ip_mask* **community** *string*

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the aggregate route.
<i>ip_mask</i>	32-bit subnet mask that determines how many bits of the IP address denote the network number.
<i>string</i>	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.

Defaults

parameter	default
<i>string</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

You can revert the aggregate community string to its default value by setting the community string to “**none**”. For example:

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 community none
```

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 community no-export  
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 community no-export
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp aggregate-address](#) Creates and deletes a BGP aggregate route.

MIB Objects

alaBgpAggrTable

alaBgpAggrAddr

alaBgpAggrMask

 alaBgpAggrCommunity

ip bgp aggregate-address local-preference

Configures the local preference attribute value for this BGP aggregate. This value will override the default local preference value; it is used when announcing this aggregate to internal peers.

ip bgp aggregate-address *ip_address ip_mask local-preference value*

no ip bgp aggregate-address *ip_address ip_mask local-preference value*

Syntax Definitions

<i>ip_address</i>	An IP address for the aggregate route.
<i>ip_mask</i>	A 32-bit subnet mask that determines how many bits of the IP address denote the network number.
<i>value</i>	The local preference attribute. The valid range is 0–4294967295

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to set the local preference back to the default value.
- You can specify that this route use the default local preference value for the AS by specifying zero (0). In this case the local preference for this route will take the default local preference value set for this AS (defined in the **ip bgp default local-preference** command).

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 local-preference 200
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 local-preference 200
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp default local-preference Sets the default local preference value for this AS.

MIB Objects

alaBgpAggrTable

alaBgpAggrAddr

alaBgpAggrMask

 alaBgpAggrLocalPref

ip bgp aggregate-address metric

Configures the MED attribute value for a BGP aggregate. This value is used when announcing this aggregate to internal peers; it indicates the best exit point from the AS.

ip bgp aggregate-address *ip_address ip_mask metric value*

no ip bgp aggregate-address *ip_address ip_mask metric value*

Syntax Definitions

<i>ip_address</i>	A 32-bit IP address.
<i>ip_mask</i>	A 32-bit subnet mask that determines how many bits of the IP address denote the network number.
<i>value</i>	The MED attribute. The valid range is 0–4294967295.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to reset the aggregate metric back to its default value.
- The default value of zero indicates that a MED will not be sent for this aggregate. When a MED value is missing for a route, BGP will determine a MED value based upon the settings specified in the **ip bgp bestpath med missing-as-worst** command.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 metric 0
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 metric 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp bestpath med missing-as-worst Configures the MED for paths that do not contain a MED value.

ip bgp always-compare-med Forces BGP to use the MED for comparison of external routes.

MIB Objects

```
alaBgpAggrTable  
  alaBgpAggrAddr  
  alaBgpAggrMask  
  alaBgpAggrMetric
```

ip bgp aggregate-address summary-only

Enables or disables aggregate summarization, which suppresses more-specific routes. Disabling aggregate summarization means that more-specific routes will be announced to BGP peers (internal and external peers).

ip bgp aggregate-address *ip_address ip_mask summary-only*

no ip bgp aggregate-address *ip_address ip_mask summary-only*

Syntax Definitions

<i>ip_address</i>	IP address for the aggregate route.
<i>ip_mask</i>	32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

This command is enabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- This command specifies whether more-specific routes should be announced or suppressed.
- By default, aggregate summarization is enabled, which means that only the aggregate entry (for example, 100.10.0.0) is advertised. Advertisements of more-specific routes (for example, 100.10.20.0) are suppressed.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 summary-only
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 summary-only
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address Creates and deletes a BGP aggregate route.

MIB Objects

alaBgpAggrTable

alaBgpAggrAddr

alaBgpAggrMask

 alaBgpAggrSummarize

ip bgp network

Creates or deletes a BGP network. A network must be known to the local BGP speaker; it also must originate from the local BGP speaker. The network may be directly connected, dynamically learned, or static.

In lieu of these options, the base command (**ip bgp network**) may be used with other keywords to set up network configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

ip bgp network *network_address ip_mask*

[**community** *string*]

[**local-preference** *value*]

[**metric** *metric*]

[**admin-state** {**enable** | **disable**}]

no ip bgp network *network_address ip_mask*

Syntax Definitions

network_address 32-bit IP address.

ip_mask 32-bit subnet mask that determines how many bits of the network address denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a local network.
- Creating and enabling a network entry indicates to BGP that this network should originate from this router. The network specified must be known to the router, whether it is connected, static, or dynamically learned.
- You can create up to 200 network entries. The basic **show ip bgp path** command will display every network currently defined.
- This command allows administrative operations on a BGP network. You must still enable the network through the **ip bgp network admin-state** command.

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0
-> no ip bgp network 172.22.2.115 255.255.255.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network admin-state Enables a BGP network.

MIB Objects

```
alaBgpNetworkTable  
  alaBgpNetworkAddr  
  alaBgpNetworkMetric  
  alaBgpNetworkLocalPref  
  alaBgpNetworkCommunity  
  alaBgpNetworkMask
```

ip bgp network admin-state

Enables or disables a BGP network.

ip bgp network *network_address ip_mask* **admin-state** {**enable** | **disable**}

Syntax Definitions

<i>network_address</i>	32-bit IP address.
<i>ip_mask</i>	32-bit subnet mask that determines how many bits of the network address denote the network number.
enable	Enables this network.
disable	Disables this network.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Configure all network parameters before enabling this BGP network with this command. Use the **ip bgp network** command to configure individual aggregate parameters.
- You can create up to 200 network entries. The **show ip bgp path** command displays every network currently defined.

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands**ip bgp network**

Create a BGP network.

show ip bgp path

Display currently defined BGP networks.

MIB Objects

alaBgpNetworkTable

alaBgpNetworkAddr

 alaBgpNetworkMask

ip bgp network community

Defines a community for a route created by the **ip bgp network** command. Communities are a way of grouping BGP peers that do not share an IP subnet or an AS.

ip bgp network *network_address ip_mask community string*

Syntax Definitions

<i>network_address</i>	32-bit IP address of the network.
<i>ip_mask</i>	32-bit subnet mask that determines how many bits of the network address denote the network number.
<i>string</i>	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.

Defaults

parameter	default
<i>string</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

You can revert the network community string to its default value by setting the community string to “**none**”. For example:

```
-> ip bgp network 172.22.2.115 255.255.255.0 community none
```

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 community export
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp network](#) Creates or deletes a BGP network

MIB Objects

alaBgpNetworkTable
 alaBgpNetworkAddr
 alaBgpNetworkMask
 alaBgpNetworkCommunity

ip bgp network local-preference

Defines the local preference value for a route generated by the **ip bgp network** command. This value will override the default local preference value; it is used when announcing this network to internal peers.

ip bgp network *network_address ip_mask local-preference value*

no ip bgp network *network_address ip_mask local-preference value*

Syntax Definitions

network_address A 32-bit IP address.

ip_mask A 32-bit subnet mask that determines how many bits of the network address denote the network number.

value The local preference attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to return the local preference of the specified network to its default setting.
- You can specify that this route use the default local preference value for the AS by specifying zero (0). In this case the local preference for this route will take the default local preference value set for this AS (defined in the **ip bgp default local-preference** command).

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 local-preference 600
-> no ip bgp network 172.22.2.115 255.255.255.0 local-preference 600
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network Creates or deletes a BGP network.

ip bgp default local-preference Sets the default local preference for this AS.

MIB Objects

```
alaBgpNetworkTable  
  alaBgpNetworkAddr  
  alaBgpNetworkMask  
  alaBgpNetworkLocalPref
```

ip bgp network metric

Configures the Multi-Exit Discriminator (MED) attribute value for an network generated by the **ip bgp network** command. This value is used when announcing this network to internal peers; it indicates the best exit point from the AS.

ip bgp network *network_address ip_mask metric value*

no ip bgp network *network_address ip_mask metric value*

Syntax Definitions

<i>network_address</i>	A 32-bit IP address.
<i>ip_mask</i>	A 32-bit subnet mask that determines how many bits of the network address denote the network number.
<i>value</i>	A MED attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to return the metric for this network to its default value.
- The default value of zero indicates that a MED will not be sent for this network. When a MED value is missing for a route, BGP will determine a MED value based upon the settings specified in the **ip bgp bestpath med missing-as-worst** command.

Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 metric 100
-> no ip bgp network 172.22.2.115 255.255.255.0 metric 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network	Creates or deletes a BGP network.
ip bgp bestpath med missing-as-worst	Specifies the MED value when it is missing.

MIB Objects

```
alaBgpNetworkTable  
  alaBgpNetworkAddr  
  alaBgpNetworkMask  
  alaBgpNetwrokMetric
```

ip bgp neighbor admin-state

Enables or disables a BGP peer.

```
ip bgp neighbor ip_address admin-state {enable | disable}
```

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the new BGP peer.
enable	Enables this peer.
disable	Disables this peer.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You must first create a peer and assign it an IP address using the **ip bgp neighbor** command before enabling the peer.
- Configure all BGP peer related commands before enabling a peer using this command. Once you enable the peer it will begin sending BGP connection and route advertisement messages.

Examples

```
-> ip bgp neighbor 172.22.2.115 admin-state enable  
-> ip bgp neighbor 172.22.2.115 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor	Creates a BGP peer.
show ip bgp neighbors	Displays peer parameters.

MIB Objects

```
alaBgpPeerTable  
  alaBgpPeerAddr
```

ip bgp neighbor advertisement-interval

Configures the time interval for updates between external BGP peers.

```
ip bgp neighbor ip_address advertisement-interval value
```

Syntax Definitions

ip_address 32-bit IP address of the neighbor.

value An advertisement time interval in seconds. The valid range is 0–65535.

Defaults

parameter	default
<i>value</i>	30

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Internal peers sharing the same AS as the local BGP speaker (configured in the [ip bgp autonomous-system](#) command) use the global route advertisement update interval. This command sets the interval this peer uses to send BGP UPDATE messages to external peers.

Examples

```
-> ip bgp neighbor 172.22.2.115 255.255.255.0 advertisement-interval 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bgp neighbors](#) Displays BGP peer main status.

MIB Objects

```
alaBgpPeerTable  
  alaBgpPeerAddr  
  bgpPeerMinRouteAdvertisementTinterval
```

Related Commands

ip bgp neighbor auto-restart Automatically attempts to restart a BGP peer session after a session terminates.

MIB Objects

alaBgpPeerTable
 alaBgpPeerAddr
 alaBgpPeerRestart

ip bgp neighbor timers

Configures the KEEPALIVE message interval and hold time interval (in seconds) with regards to the specified peer.

ip bgp neighbor *ip_address* **timers** *keepalive holdtime*

Syntax Definitions

<i>ip_address</i>	A 32-bit IP address for the BGP peer.
<i>keepalive</i>	The interval (in seconds) between KEEPALIVE messages. The valid values are zero (0) or the range 1–21845.
<i>holdtime</i>	The hold time interval between updates to peers, in seconds. The valid range is 0, 3–65535.

Defaults

parameter	default
<i>keepalive</i>	30
<i>holdtime</i>	90

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Configures the time interval between KEEPALIVE messages sent by this peer. KEEPALIVE messages do not contain route updates or indicate a change in the status of the BGP peer; they serve only to tell the receiving BGP peer that the connection is still live and the peer is reachable.
- By default, the keep alive interval of 30 seconds is one-third the default hold-time interval of 90 seconds. The keep alive interval can never be more than one-third the value of the hold-time interval. When the hold interval is reached without receiving keep alive or other updates messages, the peer is considered dead.
- Setting the keep alive value to zero means no keep alive messages will be sent.
- Once a connection is established with a peer and a time period of the length specified in this command transpires with no messages from the remote peer, then the connection with that remote peer will be considered dead.
- Configures the tolerated hold time interval, in seconds, for messages to this peer from other peers. The hold timer is used during the connection setup process and in on-going connection maintenance with BGP peers. If this peer does not receive a KEEPALIVE, UPDATE, or NOTIFICATION message within this time period, then the BGP connection will be closed.
- By default, the hold-interval of 180 seconds is three times the default keep-alive interval of 60 seconds. The hold-interval can never be less than three times the keep-alive value.

- You must restart the peer (using the **ip bgp neighbor clear** command) after issuing this command before the new hold time interval takes effect.
- Both values must be set at the same time.
- Entering this command without the variables resets the variables to their default value.

Examples

```
-> ip bgp neighbor 172.22.2.115 timers 80 240
-> ip bgp neighbor 172.22.2.115 timers
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor conn-retry-interval

The interval, in seconds, between BGP retries to set up a connection through the transport protocol with another peer.

MIB Objects

```
alaBgpPeerTable
  alaBgpPeerAddr
  bgpPeerHoldTimeConfigured
  bgpPeerKeepAliveConfigured
```

ip bgp neighbor conn-retry-interval

The interval, in seconds, between BGP retries to set up a connection through the transport protocol with another peer. In the connect state, BGP tries to set up a connection with a remote peer. If the connection fails, then the connect retry interval is started. Once this interval elapses, BGP retries setting up the connection.

ip bgp neighbor *ip_address* **conn-retry-interval** *seconds*

Syntax Definitions

<i>ip_address</i>	A 32-bit IP address for the neighbor.
<i>seconds</i>	The time interval (in seconds) between retries. The valid range is 0–65535.

Defaults

parameter	default
<i>seconds</i>	120

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The time interval is started when a connection to a peer is lost.
- Other BGP peers may automatically attempt to restart a connection with this peer if they have configured automatic peer session restart (using the **ip bgp neighbor auto-restart** command).
- You must restart the peer (using the **ip bgp neighbor clear** command) after issuing this command before the new connection retry interval takes effect.
- Entering this command without the *seconds* variable resets the variable to its default value.

Examples

```
-> ip bgp neighbor 172.22.2.115 connect-interval 60
-> ip bgp neighbor 172.22.2.115 connect-interval
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bgp neighbor auto-restart** Enable automatic session restart after a session termination.
- ip bgp neighbor clear** Restarts the peer.

MIB Objects

alaBgpPeerTable
 alaBgpPeerAddr
 bgpPeerConnectRetryInterval

Related Commands

- ip bgp neighbor** Creates a BGP peer.
ip bgp neighbor admin-state Enables a BGP peer.

MIB Objects

alaBgpPeerTable
 alaBgpPeerAddr
 alaBgpPeerAutoRestart

ip bgp neighbor maximum-prefix

Configures the maximum number of prefixes, or paths, the local router can receive from this peer in UPDATE messages.

ip bgp neighbor *ip_address* **maximum-prefix** *maximum* [**warning-only**]

Syntax Definitions

ip_address A 32-bit IP address of the BGP peer.

maximum The maximum number of prefixes. The valid range is 0–4294967295.

Defaults

parameter	default
<i>threshold</i>	5000

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When the number of prefixes sent by this peer reaches this limit, the peer is restarted.
- You can use BGP logging to receive a warning when the number of prefixes received from this peer reaches 80 percent of the value you configure in this command.
- If the **warning-only** prefix is used, the operator will be warned when the peer exceeds 80 percent of the configured number of maximum prefixes.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 maximum-prefix 1000
-> ip bgp neighbor 172.22.2.115 maximum-prefix 1000 warning only
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor clear Restarts the BGP peer.

MIB Objects

alaBgpPeerTable

 alaBgpPeerAddr

 alaBgpPeerMaxPrefixWarnOnly

 alaBgpPeerMaxPrefix

ip bgp neighbor md5 key

Sets an encrypted MD5 signature for TCP sessions with this peer in compliance with RFC 2385.

ip bgp neighbor *ip_address* **md5 key** {*string* | **none**}

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the BGP peer.
<i>string</i>	The MD5 public key. Maximum character length is 200.
none	Removes the MD5 public key.

Defaults

parameter	default
<i>string</i>	no password

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Entering the keyword **none** in place of a key removes the password and disables authentication.
- Due to security concerns the actual password that you specify in this command is encrypted using a 3DES algorithm before it appears in a saved snapshot file. Also, if you were to view this command in a snapshot file, or **boot.cfg** file, it would appear in a different syntax. The syntax for this command used for snapshot files is as follows:

ip bgp neighbor *ip_address* **md5 key-encrypt** *encrypted_string*

However, you should not use this syntax to actually set an MD5 password; it will not work.

- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 md5 key openpeer5
```

Release History

Release 7.1.1; command was introduced.

Related Commands**ip bgp neighbor clear**

Restarts the BGP peer.

MIB Objects

alaBgpPeerTable

alaBgpPeerAddr

 alaBgpPeerMD5Key

ip bgp neighbor ebgp-multihop

Allows external peers to communicate with each other even when they are not directly connected. The absence of communication between disconnected peers can occur when a router that is not running BGP sits between two BGP speakers; in such a scenario the BGP speakers are multiple hops from each other. By enabling this command, you allow the BGP peers to speak to each other despite the non-BGP router that sits between them.

ip bgp neighbor *ip_address* **ebgp-multihop** [*tth*]

no ip bgp neighbor *ip_address* **ebgp-multihop**

Syntax Definitions

ip_address 32-bit IP address of the BGP peer.

tth The Time to Live for the multi-hop connection, in seconds. The range is 1 to 255.

Defaults

parameter	default
<i>tth</i>	255

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable multi-hop connections.
- By default an external BGP peer is on a directly connected subnet. This command allows you to configure an external BGP peer that is not directly connected and may be multiple hops away. It should be used with caution and only with the guidance of qualified technical support.
- As a safeguard against loops, the multi-hop connection will not be made if the only route to a multi-hop peer is the default route (0.0.0.0).
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 ebgp-multihop 250
-> no ip bgp neighbor 172.22.2.115 ebgp-multihop 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands**ip bgp neighbor**

Creates or deletes a BGP peer.

ip bgp neighbor next-hop-self

Sets the BGP peer to use next hop processing behavior.

MIB Objects

alaBgpPeerTable

alaBgpPeerAddr

 alaBgpPeerMultiHop

ip bgp neighbor description

Configures the BGP peer name.

```
ip bgp neighbor ip_address description string
```

Syntax Definitions

ip_address 32-bit IP address of the BGP peer.
string Peer name (1 - 20 characters).

Defaults

parameter	default
<i>string</i>	peer(ip_address)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The peer name is a text identifier that, by default, follows the format “peer(x.x.x.x)” where x.x.x.x is the IP address of the BGP peer. For example, the default name of a peer at address 198.216.14.23 would be “peer(198.216.14.23)”.
- A peer name with embedded spaces must be enclosed in quotation marks.

Examples

```
-> ip bgp neighbor 172.22.2.115 description "peer for building 3"
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp neighbor](#) Sets the IP address for the peer.

MIB Objects

```
alaBgpPeerTable  
  alaBgpPeerAddr  
  alaBgpPeerName
```

ip bgp neighbor next-hop-self

Sets the BGP peer to use next hop processing behavior. By default, the next-hop processing of BGP updates is disabled. Using this command to enable next-hop behavior may be useful in non-meshed networks where BGP peers do not have direct access to other peers.

ip bgp neighbor *ip_address* next-hop-self

no ip bgp neighbor *ip_address* next-hop-self

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable next hop processing behavior.
- In partially meshed networks a BGP peer may not have direct connections to other peers. When such a peer receives route updates from these distant peers (through other peers), it may treat the remote peer as if it were the next hop in the routing path. Packet forwarding will not work in such a case because no direct connection exists. This command allows this peer to deem itself the next hop on the routing path so that the two non-connected peers can route packets. This peer would have a direct connection to both peers that want to exchange packets.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 next-hop-self  
-> no ip bgp neighbor 172.22.2.115 next-hop-self
```

Release History

Release 7.1.1; command was introduced.

Related Commands**ip bgp neighbor**

Creates or deletes a BGP peer.

MIB Objects

alaBgpPeerTable

alaBgpPeerAddr

 alaBgpPeerNextHopSelf

ip bgp neighbor remote-as

Assigns an AS number to this BGP peer.

```
ip bgp neighbor ip_address remote-as value
```

Syntax Definitions

ip_address 32-bit IP address of the BGP peer.

value Autonomous system number in the range 1 - 65535.

Defaults

parameter	default
<i>value</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A BGP peer created with the **ip bgp neighbor** command cannot be enabled (**ip bgp neighbor admin-state enable**) until it is assigned an autonomous system number. If the AS number matches the AS number assigned to the local BGP speaker (assigned using the **ip bgp autonomous-system** command), the peer is considered internal to the local autonomous system. Otherwise, the peer is considered external to the local BGP speaker's AS.
- This BGP peer may not be operational within this router and it may be in an external AS, but it must still be configured on this router before the local BGP speaker can establish a connection to the peer. The local BGP speaker does not auto-discover peers in other routers; it initially learns about peers through the peer commands.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 remote-as 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp autonomous-system	Set the AS for the local BGP speaker.
ip bgp neighbor	Create a BGP peer.
ip bgp neighbor admin-state enable	Enables a BGP peer.

MIB Objects

alaBgpPeerTable
 alaBgpPeerAddr
 alaBgpPeerAS

ip bgp neighbor remove-private-as

Enables or disables the stripping of private autonomous system numbers from the AS path of routes destined to this peer.

ip bgp neighbor *ip_address* remove-private-as

no ip bgp neighbor *ip_address* remove-private-as

Syntax Definitions

ip_address 32-bit IP address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable stripping of private AS numbers.
- By default all AS numbers in the AS path are passed to peers. Enabling this command strips any private AS numbers in the AS path before sending updates to this peer. AS numbers in the range 64512 to 65535 are considered private ASs; they intended for internal use within an organization (such as an enterprise network), but they are not intended for use on public networks (such as the Internet).
- This command has no effect if you are not using ASs in the range 64512 to 65535.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 remove-private-as
-> no ip bgp neighbor 172.22.2.115 remove-private-as
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor remote-as Configures the AS number for this peer.

MIB Objects

```
alaBgpPeerTable
  alaBgpPeerAddr
  alaBgpPeerRemovePrivateAs
```

ip bgp neighbor soft-reconfiguration

Enables or disables BGP peer soft reconfiguration. Soft reconfiguration increases the stability of the peer by allowing you to reconfigure attributes that require peer resets without halting the TCP connection with other peers.

ip bgp neighbor *ip_address* soft-reconfiguration

no ip bgp neighbor *ip_address* soft-reconfiguration

Syntax Definitions

ip_address 32-bit IP address of the BGP peer.

Default

This command is enabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- This feature stores routes and other configuration information in local memory. When you make configuration changes that require a peer reset, the routing cache is not cleared and connections with other peers are not interrupted.
- By default BGP stores all paths from peers, even those that are policy rejected, in anticipation of policy changes in the future. Storing these paths consumes memory. You can use this command to disable the storing of these paths, or soft reconfiguration. However, if soft reconfiguration is disabled and the inbound policy changes, the peer will have to be restarted using the [ip bgp neighbor out-aspalists](#) command.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp neighbor 172.22.2.115 soft-reconfiguration
-> no ip bgp neighbor 172.22.2.115 soft-reconfiguration
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bgp neighbor clear** Restarts this BGP peer.
- ip bgp neighbor out-asp-pathlist** Resets inbound policies to this peer.

MIB Objects

alaBgpPeerTable
 alaBgpPeerAddr
 alaBgpPeerSoftReconfig

ip bgp neighbor stats-clear

Clears the statistics for a peer.

ip bgp neighbor *ip_address* stats-clear

Syntax Definitions

ip_address 32-bit IP address of the BGP peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command clears the statistical variables for a peer so they can accumulate from a known point.
- The cleared statistics include the total messages sent and received from this peer, the total UPDATE messages sent and received from this peer, the total NOTIFY messages sent and received from this peer, and the total peer state transition messages sent and received from this peer. These statistics can be displayed through [show ip bgp neighbors statistics](#).

Examples

```
-> ip bgp neighbor 172.22.2.115 stats-clear
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bgp neighbors statistics](#) Displays peer statistics.

MIB Objects

```
alaBgpPeerTable  
  alaBgpPeerAddr  
  alaBgpPeerClearCounter
```

ip bgp confederation neighbor

Configures this peer as a member of the same confederation as the local BGP speaker.

ip bgp confederation neighbor *ip_address*

no ip bgp confederation neighbor *ip_address*

Syntax Definitions

ip_address 32-bit IP address of the peer.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- You must first assign a confederation number to the local BGP speaker before assigning peers to the confederation. Use the **ip bgp confederation identifier** command to assign a confederation number to the local BGP speaker.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ip bgp confederation neighbor 172.22.2.115
-> no ip bgp confederation neighbor 172.22.2.115
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp confederation identifier Sets a confederation identification value for the local BGP speaker (this router).

MIB Objects

alaBgpPeerTable
 alaBgpPeerAddr
 alaBgpPeerConfedStatus

ip bgp neighbor update-source

Configures the local address from which this peer will be contacted. This local address can be configured for internal and external BGP peers.

```
ip bgp neighbor ip_address update-source [interface_name]
```

Syntax Definitions

ip_address The 32-bit IP address for this peer.

interface_name The name of the interface.

Defaults

parameter	default
<i>interface_address</i>	0.0.0.0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This address does not override the router identification for this BGP peer (configured in the **ip bgp neighbor** command). It is the address through which this peer can be contacted within this router. The router identification for a peer, especially an external peer, may not exist in the local router, but that distant peer can still be contacted through this router. This command sets the local address through which this distant peer can be contacted.
- The default is restored by entering the command without a IP address.
- The BGP peer is restarted after issuing this command.
- The update-source is not related to the router-id, it specifies the interface to be used for the TCP connection endpoint. By default, the nearest interface is selected.

Examples

```
-> ip bgp neighbor 172.22.5.115 update-source 172.22.2.117
-> ip bgp neighbor 172.22.5.115 update-source vlan-22
-> ip bgp neighbor 172.22.5.115 update-source
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor

Sets the router identification for a BGP peer.

MIB Objects

alaBgpPeerTable

 alaBgpPeerAddr

 alaBgpPeerLocalAddr

 alaBgpPeerLocalIntfName

ip bgp neighbor in-aspathlist

Assigns an inbound AS path list filter to a BGP peer.

ip bgp neighbor *ip_address* **in-aspathlist** {*string* / **none**}

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the BGP peer.
<i>string</i>	Inbound AS path list (0 to 70 characters). This name is case sensitive.
none	Removes this AS path list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The AS path list name (**InboundASpath** in the example below) is created using the [ip bgp policy aspath-list](#) command. Any inbound routes from the BGP peer must match this AS path filter before being accepted or passed to inbound policy.
- To deassign an input AS path filter list, use this command to assign a value of **none**.

Examples

```
-> ip bgp neighbor 172.22.2.115 in-aspathlist InboundASpath
-> ip bgp neighbor 172.22.2.115 in-aspathlist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy aspath-list](#) Creates or removes an AS path list.

MIB Objects

alaBgpPeerTable
alaBgpPeerAspathListIn

ip bgp neighbor in-communitylist

Assigns an inbound community list filter to a BGP peer.

```
ip bgp neighbor ip_address in-communitylist {string / none}
```

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the BGP peer.
<i>string</i>	Input community list (0 to 70 characters. This name is case sensitive).
none	Removes this community list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The community filter list name (**InboundCommlist** in the example below) is created using the **ip bgp policy community-list** command. Any inbound routes from the BGP peer must match this community filter before being accepted or passed to inbound policy.
- To deassign an input community filter list, use this command to assign a value of “**none**.”

Examples

```
-> ip bgp neighbor 172.22.2.115 in-communitylist InboundCommlist  
-> ip bgp neighbor 172.22.2.115 in-communitylist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy community-list Creates or deletes a community list.

MIB Objects

```
alaBgpPeerTable  
  alaBgpPeerCommunityListIn
```

ip bgp neighbor in-prefixlist

Assigns an inbound prefix filter list to a BGP peer.

```
ip bgp neighbor ip_address in-prefixlist {string / none}
```

Syntax Definitions

<i>ip_address</i>	32-bit IP address.
<i>string</i>	Input prefix filter list (0 to 70 characters). This name is case sensitive.
none	Removes the prefix list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The prefix list name (**InboundPrefix** in the example below) is created using the [ip bgp policy prefix-list](#) command. Any inbound routes from the BGP peer must match this prefix filter before being accepted or passed to inbound policy.
- To deassign an input prefix filter list, use this command to assign a value of “**none.**”

Examples

```
-> ip bgp neighbor 172.22.2.115 in-prefixlist InboundPrefix  
-> ip bgp neighbor 172.22.2.115 in-prefixlist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix-list](#) Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeerTable  
  alaBgpPeerPrefixListIn
```

ip bgp neighbor out-aspathlist

Assigns an outbound AS path filter list to a BGP peer.

```
ip bgp neighbor ip_address out-aspathlist {string / none}
```

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the BGP peer.
<i>string</i>	Outbound AS path list (0 - 70 characters).
none	Removes the AS path list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The AS path list name (**OutboundASpath** in the example below) is created using the [ip bgp policy aspath-list](#) command. Any outbound routes from the BGP peer must match this AS path filter, or policy, before being advertised or passed to outbound policy.
- To deassign an output AS path filter list, use this command to assign a value of “**none**”.

Examples

```
-> ip bgp neighbor 172.22.2.115 out-aspathlist OutboundASpath
-> ip bgp neighbor 172.22.2.115 out-aspathlist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy aspath-list](#) Creates or removes an AS path list.

MIB Objects

```
alaBgpPeerTable
  alaBgpPeerAspathListOut
```

ip bgp neighbor out-communitylist

Assigns an outbound community filter list to a BGP peer.

```
ip bgp neighbor ip_address out-communitylist {string | none}
```

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the BGP peer.
<i>string</i>	Outbound community list (0 - 70 characters).
none	Removes the community list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The community filter list name (**OutboundCommlist** in the example below) is created using the **ip bgp policy community-list** command. Any outbound routes from the BGP peer must match this community filter before being advertised or passed to outbound policy.
- To deassign an output community filter list, use this command to assign a value of “**none**”.

Examples

```
-> ip bgp neighbor 172.22.2.115 out-communitylist OutboundCommlist  
-> ip bgp neighbor 172.22.2.115 out-communitylist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy community-list Creates or deletes a community list.

MIB Objects

```
alaBgpPeerTable  
  alaBgpPeerCommunityListOut
```

ip bgp neighbor out-prefixlist

Assigns an outbound prefix filter list to a BGP peer.

```
ip bgp neighbor ip_address out-prefixlist {string / none}
```

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the BGP peer.
<i>string</i>	Output prefix filter list (0 - 70 characters).
none	Removes the prefix list from the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The prefix list name (**OutboundPrefix** in the example below) is created using the [ip bgp policy prefix-list](#) command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to outbound policy.
- To deassign an output prefix filter list, use this command to assign a value of “**none**”.

Examples

```
-> ip bgp neighbor 172.22.2.115 out-prefixlist OutboundPrefix
-> ip bgp neighbor 172.22.2.115 out-prefixlist none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix-list](#) Creates or deletes a prefix match list.

MIB Objects

```
alaBgpPeerTable
  alaBgpPeerPrefixListOut
```

ip bgp neighbor route-map

Assigns an inbound policy map to a BGP peer.

```
ip bgp neighbor ip_address route-map {string | none} {in | out}
```

```
no ip bgp neighbor ip_address route-map {in | out}
```

Syntax Definitions

<i>ip_address</i>	32-bit IP address of the peer.
<i>string</i>	Inbound policy map name (0 to 70 characters). This name is case sensitive.
none	Deletes the route map if entered rather than a text string.
in	Designates this route map policy as an inbound policy.
out	Designates this route map policy as an outbound policy.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to deassign an inbound map.
- The policy route map name (**peeringPointAMap** in the example below) is created using the **ip bgp policy prefix6-list** command. Any inbound routes from the BGP peer must match this route map filter before being accepted or passed to inbound policy.
- It is also possible to deassign a route map by entering **none** in place of a route map name.

Examples

```
-> ip bgp neighbor 172.22.2.115 route-map InboundRoute in
-> ip bgp neighbor 172.22.2.115 route-map OutboundRoute out
-> ip bgp neighbor 172.22.2.115 route-map none in
-> no ip bgp neighbor 172.22.2.115 route-map in
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#) Creates or deletes a policy route map.

MIB Objects

```
alaBgpPeerTable
  alaBgpPeerRouteMapOut
  alaBgpPeerRouteMapIn
```

ip bgp neighbor clear soft

Invokes an inbound or outbound policy reconfiguration for a BGP peer.

ip bgp neighbor *ip_address* **clear soft** {**in** | **out**}

Syntax Definitions

<i>ip_address</i>	32-bit IP address for the BGP peer.
in	Applies reconfiguration to the inbound policies.
out	Applies reconfiguration to the outbound policies.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command reconfigures (or reapplies) all inbound or outbound policies to existing routes without restarting the peer session.
- This command is useful if policies have been changed.

Examples

```
-> ip bgp neighbor 172.22.2.115 clear soft in
-> ip bgp neighbor 172.22.2.115 clear soft out
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp neighbor soft-reconfiguration](#) Enables or disables BGP peer soft reconfiguration.

MIB Objects

```
alaBgpPeerTable
  alaBgpPeerReconfigureInBound
  alaBgpPeerReconfigureOutBound
```

ip bgp policy aspath-list

Creates or removes an AS path list.

ip bgp policy aspath-list *name* “*regular_expression*”

no ip bgp policy aspath-list *name* “*regular_expression*”

Syntax Definitions

<i>name</i>	AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
<i>regular_expression</i>	Regular expression, e.g., “^100 200\$” where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.

Defaults

No IP BGP peer policy AS path-list exists.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove an AS path list.
- To create an AS path list, use the **ip bgp policy aspath-list** command.
- A regular expression consists of a character string presented in the form of a pattern, e.g., ^100 200\$. Valid regular expression characters (metacharacters) are shown in the table below. See also “Configuring BGP” in your Advanced Routing Guide for more information on using regular expressions in BGP commands.

Symbol	Description
^	Matches the beginning of the AS path list.
123	Matches the AS number 123.
.	Matches any single AS number.
?	Matches zero or one occurrence of the previous token, which must be an AS number, a dot, an alternation or a range.
+	Matches one or more occurrences of the previous token, which must be an AS number, a dot, an alternation or a range.
*	Matches zero or more occurrences of the previous token, which must be an AS number, a dot, an alternation or a range.
(Begins an alternation sequence of AS numbers. It matches any AS number listed in the alternation sequence.

Symbol	Description
	Separates AS numbers in an alternation sequence.
)	Ends an alternation sequence of AS numbers
[Begins a range pair consisting of two AS numbers separated by a dash. It matches any AS number within that inclusive range.
-	Separates the endpoints of a range.
]	Ends a range pair.
\$	Matches the end of the AS path list.
,_	Commas, underscores and spaces are ignored.

- When using a regular expression in the CLI, the regular expression must be enclosed in quotation marks.
- This command creates AS path lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-[aspathlist](#)** and **ip bgp neighbor out-[aspathlist](#)** commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies.
- If a BGP AS path list is configured to deny routes from a particular string of regular expression, then by default all of the routes coming from any AS would be denied. You must configure the policy instance in the same policy to allow other routes to come in, to be permitted from other ASs.
- General or more specific AS path list information can be displayed by varying the use of the **show ip [bgp](#)** command.

Examples

```
-> ip bgp policy aspath-list InboundAspath "^100 200$"
-> ip bgp policy aspath-list OutboundAspath "^300 400$"
-> no ip bgp policy aspath-list InboundAspath "^100 200$"
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor out-aspathlist	Assigns an outbound AS path list filter to a BGP peer.
ip bgp policy aspath-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found.
ip bgp policy aspath-list priority	Configures priority for processing regular expressions in an AS path list.

MIB Objects

alaBgpAspathMatchListTable
 alaBgpAspathMatchListRowStatus

ip bgp policy aspath-list action

Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found. Matching criteria are specified in the regular expression.

ip bgp policy aspath-list *name* "*regular_expression*" **action** {**permit** | **deny**}

Syntax Definitions

<i>name</i>	AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
<i>regular_expression</i>	Regular expression, e.g., " ^100 200\$ " where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A regular expression consists of a character string presented in the form of a pattern, e.g., **^100 200\$**. Refer to [ip bgp policy aspath-list](#) on page 22-96 for a table of valid regular expression characters (metacharacters). See also "Configuring BGP" in your Advanced Routing Guide for more information on using regular expressions in BGP commands.
- This command allows or stops AS path lists from being applied to a peer's inbound and outbound routes configured through the [ip bgp neighbor in-aspathlist](#) and [ip bgp neighbor out-aspathlist](#) commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies.
- General or more specific AS path list information can be displayed by varying the use of the [show ip bgp](#) command.

Examples

```
-> ip bgp policy aspath-list InboundAspath "^100 200$" action permit
-> ip bgp policy aspath-list OutboundAspath "^300 400$" action deny
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-aspathlist	Assigns an inbound AS path list filter to a BGP peer.
ip bgp neighbor out-aspathlist	Assigns an outbound AS path list filter to a BGP peer.
ip bgp policy aspath-list	Creates or removes an AS path list.
ip bgp policy aspath-list priority	Configures priority for processing regular expressions in an AS path list.

MIB Objects

```
alaBgpAspathMatchListTable  
    alaBgpAspathMatchListAction
```

ip bgp policy aspath-list priority

Configures the priority for processing regular expressions in an AS path list.

ip bgp policy aspath-list *name* "*regular_expression*" **priority** *value*

Syntax Definitions

<i>name</i>	The AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
<i>regular_expression</i>	A regular expression, e.g., "^100 200\$" where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.
<i>value</i>	A priority value, e.g., 1, assigned to the policy action. Valid priority range is from 1 - 255.

Defaults

parameter	default
<i>value</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A regular expression consists of a character string presented in the form of a pattern, e.g., ^100 200\$. Refer to [ip bgp policy aspath-list](#) on page 22-96 for a table of valid regular expression characters (metacharacters). See also "Configuring BGP" in your Advanced Routing Guide for more information on using regular expressions in BGP commands.
- This command specifies the priority of an AS path list filter being applied to a peer's inbound and outbound routes configured through the [ip bgp neighbor in-aspathlist](#) and [ip bgp neighbor out-aspathlist](#) commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the *permit* or *deny* action (i.e., policy) associated with the regular expression applies, but only in the order designated by the priority value.
- The higher the priority value specified in the command, the later the matching is processed. For example, regular expressions with a priority of 1 (the default) are processed before an expression assigned a priority of 3. When regular expressions have an equal priority, the processing order is indeterminate.
- General or more specific AS path list information can be displayed by varying the use of the [show ip bgp](#) command.

Examples

```
-> ip bgp policy aspath-list InboundAspath "^100 200$" priority 1
-> ip bgp policy aspath-list OutboundAspath "^300 400$" priority 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|---|--|
| ip bgp neighbor in-aspulist | Assigns an inbound AS path list filter to a BGP peer. |
| ip bgp neighbor out-aspulist | Assigns an outbound AS path list filter to a BGP peer. |
| ip bgp policy aspath-list | Creates or removes an AS path list. |
| ip bgp policy aspath-list action | Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found. |

MIB Objects

alaBgpAspathMatchListTable
 alaBgpAspathMatchListPriority

ip bgp policy community-list

Creates or deletes a community list.

ip bgp policy community-list *name* {**none** | **no-export** | **no-advertise** | **no-export-subconfed** | *num:num*}

no ip bgp policy community-list *name* {**none** | **no-export** | **no-advertise** | **no-export-subconfed** | *num:num*}

Syntax Definitions

<i>name</i>	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
<i>num:num</i>	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.

Defaults

No IP BGP peer policy community-list exists.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a community-list.
- This command creates community lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-communitylist** and **ip bgp neighbor out-communitylist** commands. The community list filters routes based on one or more community match list strings, as shown in the example below. If the route matches the community list filter, according to the matching type *exact* or *occur*, then the *permit* or *deny* policy action associated with the match list string applies.
- General or more specific community list information can be displayed by varying the use of the **show ip bgp** command.

Examples

```
-> ip bgp policy community-list CommListAIn 40:40
-> ip bgp policy community-list CommListAOut 400:20
-> ip bgp policy community-list none
-> no ip bgp policy community-list CommListAIn 400:20
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list match-type	Configures type of matching to be performed with a community string list.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.

MIB Objects

alaBgpCommunityMatchListTable
alaBgpCommunityMatchListRowStatus

ip bgp policy community-list action

Configures the action to be taken for a community list when a match is found.

ip bgp policy community-list *name* {**none** | **no-export** | **no-advertise** | **no-export-subconfed** | *num:num*}
action {**permit** | **deny**}

Syntax Definitions

<i>name</i>	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
<i>num:num</i>	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

By default, this command allows routes that match the criteria specified in the community list to pass.

Examples

```
-> ip bgp policy community-list commListAIn 600:1 action permit
-> ip bgp policy community-list commListAIn 600:1 action deny
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list match-type	Configures type of matching to be performed with a community string list.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.

MIB Objects

alaBgpCommunityMatchListTable
alaBgpCommunityMatchListAction

ip bgp policy community-list match-type

Configures the type of matching to be performed with a community string list.

ip bgp policy community-list *name* {**none** | **no-export** | **no-advertise** | **no-export-subconfed** | *num:num*}
match-type {**exact** | **occur**}

Syntax Definitions

<i>name</i>	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
<i>num:num</i>	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
exact	Checks for an exact match of the community string and the community attribute.
occur	Checks for an occurrence of the community string anywhere in the community attribute.

Defaults

parameter	default
exact occur	exact

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

By default, this command only allows routes to pass if the community string exactly matches the community attribute of the route.

Examples

```
-> ip bgp policy community-list commListC 600:1 match-type exact
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor in-communitylist	Assigns an inbound AS community list filter to a BGP peer.
ip bgp neighbor out-communitylist	Assigns an outbound AS community list filter to a BGP peer.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list priority	Configures priority for processing multiple items in a community list filter.

MIB Objects

alaBgpCommunityMatchListTable
alaBgpCommunityMatchListType

ip bgp policy community-list priority

Configures the priority for processing multiple items in a community list filter.

ip bgp policy community-list *name* {**none** | **no-export** | **no-advertise** | **no-export-subconfed** | *num:num*}
priority *value*

Syntax Definitions

<i>name</i>	Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
<i>num:num</i>	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
<i>value</i>	Priority value in the range 0 - 255.

Defaults

parameter	default
<i>value</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The higher the priority value specified in the command, the later the matching is processed. For example, items with a priority of 1 (the default) are processed before items assigned a priority of 3. When items have an equal priority, the processing order is indeterminate.

Examples

```
-> ip bgp policy community-list commListB 500:1 priority 3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy community-list	Creates or deletes a community list.
ip bgp policy community-list action	Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
ip bgp policy community-list match-type	Configures type of matching to be performed with community string list.

MIB Objects

```
alaBgpCommunityMatchListTable  
  alaBgpCommunityMatchListPriority
```

ip bgp policy prefix-list

Creates or deletes a prefix match list.

ip bgp policy prefix-list *name ip_address ip_mask*

no ip bgp policy prefix-list *name ip_address ip_mask*

Syntax Definitions

<i>name</i>	Prefix list name.
<i>ip_address</i>	IP address for the prefix list.
<i>ip_mask</i>	Mask for the prefix list.

Defaults

No IP BGP policy prefix-list exists.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command creates prefix lists that can be applied to a peer's inbound and outbound routes using the **ip bgp neighbor in-prefixlist** and **ip bgp neighbor out-prefixlist** commands. The prefix list filters routes based on one or more prefixes, as shown in the example below. If the route matches the prefix list filter, according to the **ge** (lower) and **le** (upper) limits defined, then the **permit** or **deny** action associated with the prefix applies.
- General or more specific prefix list information can be displayed by varying the use of the **show ip bgp** command.

Examples

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bgp policy prefix-list action** Configures action to be taken for a prefix list when a match is found.
- ip bgp policy prefix-list ge** Configures lower limit on length of prefix to be matched.
- ip bgp policy prefix-list le** Configures upper limit on length of prefix to be matched.

MIB Objects

alaBgpPrefixMatchListTable
 alaBgpPrefixMatchListRowStatus

ip bgp policy prefix-list action

Configures the action to be taken for a prefix list when a match is found.

ip bgp policy prefix-list *name ip_address ip_mask* **action** {**permit** | **deny**}

Syntax Definitions

<i>name</i>	Prefix list name.
<i>ip_address</i>	IP address of the prefix list.
<i>ip_mask</i>	Mask for the prefix list.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing.

Defaults

parameter	default
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Configures the action to be taken for a prefix list when a match is found.

Examples

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0 action deny
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list	Creates or deletes a prefix match list.
ip bgp policy prefix-list ge	Configures lower limit on length of prefix to be matched.
ip bgp policy prefix-list le	Configures upper limit on length of prefix to be matched.

MIB Objects

alaBgpPrefixMatchListTable
 alaBgpPrefixMatchListAction

ip bgp policy prefix-list ge

Configures the lower limit on the length of the prefix to be matched.

ip bgp policy prefix-list *name ip_address ip_mask ge value*

Syntax Definitions

<i>name</i>	Prefix list name.
<i>ip_address</i>	IP address of the prefix list.
<i>ip_mask</i>	Mask of the prefix list.
<i>value</i>	The lower limit value in the range 0 to 32.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The default value of zero indicates there is no lower limit on the length of the prefix to be matched.
- This command is used in conjunction with the **ip bgp policy prefix-list le** command to set the prefix matching range. The two commands can be combined, as show in the Example section below.
- The **ge** (lower limit) value must be greater than or equal to the prefix length (8 in the example below) and less than or equal to the **le** (upper limit) value.

Examples

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|---|--|
| ip bgp policy prefix-list | Creates or deletes a prefix match list. |
| ip bgp policy prefix-list action | Configures action to be taken for a prefix list when a match is found. |
| ip bgp policy prefix-list le | Configures upper limit on length of prefix to be matched. |

MIB Objects

```
alaBgpPrefixMatchListTable  
  alaBgpPrefixMatchListGE
```

ip bgp policy prefix-list le

Configures the upper limit on the length of the prefix to be matched.

ip bgp policy prefix-list *name ip_address ip_mask le value*

Syntax Definitions

<i>name</i>	Prefix list name.
<i>ip_address</i>	Prefix list IP address for the prefix list.
<i>ip_mask</i>	Prefix list mask for the prefix list.
<i>value</i>	The upper limit value in the range of 0 to 32.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The default value of zero indicates there is no upper limit on the length of the prefix to be matched. This command is used in conjunction with **ip bgp policy prefix-list ge** to set the prefix matching range. The two commands can be combined, as show in the Example section below.
- The **ge** (lower limit) value must be greater than or equal to the prefix length (8 in the example below) and less than or equal to the **le** (upper limit) value.

Examples

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bgp policy prefix-list** Creates or deletes a prefix match list.
- ip bgp policy prefix-list action** Configures action to be taken for a prefix list when a match is found.
- ip bgp policy prefix-list ge** Configures lower limit on length of prefix to be matched.

MIB Objects

alaBgpPrefixMatchListTable
alaBgpPrefixMatchListLE

ip bgp policy prefix6-list

Configures a BGP prefix6-list policy for filtering IPv6 prefixes. This policy can be applied to filter unique local IPv6 addresses.

```
ip bgp policy prefix6-list px_list_name prefix6/pfx_length [action{permit|deny}] [admin-state{enable|disable}] [ge{masklength}] [le{masklength}]
```

```
no ip bgp policy prefix6-list px_list_name prefix6/pfx_length [action{permit|deny}] [admin-state{enable|disable}] [ge{masklength}] [le{masklength}]
```

Syntax Definitions

<i>px_list_name</i>	Prefix list name.
<i>prefix6</i>	Prefix list IPv6 address for the prefix list.
<i>pfx_length</i>	Prefix length. Prefix length should be in the range of 0 to 128.
permit deny	Action to be taken which can be either permit or deny.
enable disable	Row Status can be either enabled or disabled.
<i>masklength</i>	Minimum length of the prefix to be matched. It should be in the range of 0 - 32.
<i>masklength</i>	Maximum length of the prefix to be matched. It should be in the range of 0 - 32.

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable this feature.
- BGP must be configured on the system.
- The **ge** (lower limit) value must be greater than or equal to the prefix length and less than or equal to the **le** (upper limit) value.

Examples

```
-> ip bgp policy prefix6-list uniqLocal FC00::/48
-> ip bgp policy prefix6-list uniqLocal FC00::/48 action permit
-> ip bgp policy prefix6-list uniqLocal FC00::/48 admin-state enable
-> no ip bgp policy prefix6-list uniqLocal FC00::/48
```


Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp policy route-map Displays configured prefix6-list policies on the system.

show ipv6 bgp neighbors Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPrefix6MatchListTable
  alaBgpPrefix6MatchListId
  alaBgpPrefix6MatchListAddr
  alaBgpPrefix6MatchListAddrLength
  alaBgpPrefix6MatchListAction
  alaBgpPrefix6MatchListRowStatus
  alaBgpPrefix6MatchListGE
  alaBgpPrefix6MatchListLE
```

ip bgp policy route-map

Creates or deletes a policy route map.

ip bgp policy route-map *name sequence_number*

Syntax Definitions

<i>name</i>	Route map name. Case-sensitive.
<i>sequence_number</i>	Route map sequence number in the range of 1 to 255. The sequence number allows for multiple instances of the same route map name.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command creates policy route maps. Each route map can be configured using the following match commands to specify the match criteria by which routes are allowed to pass. Match criteria is examined in the order the commands are listed below.
 1. **ip bgp policy route-map aspath-list**
 2. **ip bgp policy route-map prefix-list**
 3. **ip bgp policy route-map community-list**
 4. **ip bgp policy route-map match-regexp**
 5. **ip bgp policy route-map match-prefix**
 6. **ip bgp policy route-map match-mask**
 7. **ip bgp policy route-map match-community**
- Each route map can also be configured using the following set commands to sequentially specify the actions to be taken when a match is found.
 - **ip bgp policy route-map community**
 - **ip bgp policy route-map community-mode**
 - **ip bgp policy route-map lpref**
 - **ip bgp policy route-map lpref-mode**
 - **ip bgp policy route-map med**
 - **ip bgp policy route-map med-mode**
 - **ip bgp policy route-map origin**

- [ip bgp policy route-map weight](#)
- Route maps can be referenced as a filtering mechanism for displaying paths using the [show ip bgp path](#) command. They are also referenced in filtering inbound and outbound routes for BGP peers using the [ip bgp neighbor route-map](#) commands.

Examples

```
-> ip bgp policy route-map routemap1 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy route-map action](#) Configures action to be taken for a route when a match is found.

MIB Objects

```
alaBgpRouteMapTable  
  alaBgpRouteMapRowStatus
```

ip bgp policy route-map action

Configures the action to be taken for a route when a match is found.

ip bgp policy route-map *name sequence_number* **action** {**permit** | **deny**}

Syntax Definitions

<i>name</i>	A route map name.
<i>sequence_number</i>	A route map sequence number. The valid range is 1–255.
permit	Allows matching routes to pass.
deny	Stops matching routes from passing. In addition, no further instances (sequence numbers) of the route map are examined.

Defaultst

parameter	default
permit deny	permit

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

By default, this command allows routes that match the criteria specified in the route map to pass. If no matching routes are found, any additional instances (sequence numbers) of the route map name are examined. When all instances have been examined with no match, the route is dropped.

Examples

```
-> ip bgp policy route-map routemap1 1 action deny
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#) Creates or deletes a policy route map.

MIB Objects

alaBgpRouteMapTable
alaBgpRouteMapAction

ip bgp policy route-map aspath-list

Assigns an AS path matching list to the route map.

ip bgp policy route-map *name sequence_number aspath-list as_name*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>as_name</i>	The AS path list name or “none”.

Defaults

parameter	default
<i>as_name</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- By default, no AS path list is assigned to a route map.
- This default behavior can be reset by changing the value of the AS path list name to “**none**”.
- The **ip bgp policy aspath-list** and **ip bgp policy aspath-list action** commands are used to create and set permit/deny actions for an AS path list.

Examples

```
-> ip bgp policy route-map routemap1 1 aspath-list aspathlist1
-> ip bgp policy route-map routemap1 1 aspath-list none
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list Creates or deletes a policy route map.

MIB Objects

alaBgpRouteMapTable
alaBgpRouteMapAsPathMatchListId

ip bgp policy route-map asprepend

Configures the AS path prepend action to be taken when a match is found.

ip bgp policy route-map *name* *sequence_number* **asprepend** *path*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>path</i>	The AS path to prepend or “none”. Note that multiple AS path entries must be enclosed in quotes (e.g., “500 600 700”).

Defaults

parameter	default
<i>path</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

By default, no AS path is prepended. This command allows AS path numbers to be prepended (added to the beginning of the AS path list) to the AS path attribute of a matching route. The default behavior can be reset by changing the value to “none”.

Examples

```
-> ip bgp policy route-map routemap1 1 asprepend "700 800 900"
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#) Creates or deletes a policy route map.

MIB Objects

alaBgpRouteMapTable
 alaBgpRouteMapAsPrepend

ip bgp policy route-map community

Configures the action to be taken on the community attribute when a match is found.

ip bgp policy route-map *name sequence_number* **community** [**none** | **no-export** | **no-advertise** | **no-export-subconfed** | *num:num*]

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
none	Removes the community restrictions on the community section of the route map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes in this community are not advertised to any peer.
no-export-subconfed	Routes in this community are not advertised to any external BGP peer.
<i>num:num</i>	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.

Defaults

parameter	default
<i>string</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- By default, no action is taken on a community attribute when a match on a route is found.
- The default behavior can be reset by setting the value to “**none**”.
- The **ip bgp policy community-list** and **ip bgp policy community-list action** commands are used to create and set permit/deny actions for a community path list. This command is used in conjunction with **ip bgp policy route-map community-mode**.

Examples

```
-> ip bgp policy route-map routemap1 1 community 400:1 500:1
-> ip bgp policy route-map routemap1 1 community 400:1 500:1 community-mode replace
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#)

Creates or deletes a policy route map.

[ip bgp policy route-map community-mode](#)

Configures the action to be taken for a community string when a match is found.

MIB Objects

alaBgpRouteMapTable

alaBgpRouteMapCommunity

ip bgp policy route-map community-list

Assigns a community matching list to the route map.

ip bgp policy route-map *name* *sequence_number* **community-list** *name*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>name</i>	The community list name, or “none”.

Defaults

parameter	default
<i>name</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

By default, no community list is assigned to the route map. The default behavior can be reset by changing the value to “**none**”.

Examples

```
-> ip bgp policy route-map routemap1 1 community-list listB
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#) Creates or deletes a policy route map.

MIB Objects

alaBgpRouteMapTable
 alaBgpRouteMapCommunityMatchListId

ip bgp policy route-map community-mode

Configures the action to be taken for a community string when a match is found.

ip bgp policy route-map *name sequence_number* **community-mode** {**add** | **replace**}

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
add	Adds the community string specified in the command ip bgp policy route-map community .
replace	Replaces the community string specified in the command ip bgp policy route-map community .

Defaults

parameter	default
add replace	add

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command is used in conjunction with **ip bgp policy route-map community**. The example on the next line shows the combined usage.

Examples

```
-> ip bgp policy route-map routemap1 1 community-mode replace
-> ip bgp policy route-map routemap1 1 community 400:1 500:1 community-mode replace
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#)

Creates or deletes a policy route map.

[ip bgp policy route-map community](#)

Configures the action to be taken on the community attribute when a match is found.

MIB Objects

alaBgpRouteMapTable

alaBgpRouteMapSetCommunityMode

ip bgp policy route-map lpref

Configures the local preference value for the route map.

ip bgp policy route-map *name sequence_number lpref value*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>value</i>	The local preference value. The valid range is 0–4294967295

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used in conjunction with [ip bgp policy route-map lpref-mode](#). The example on the next line shows the combined usage.
- In this example, the local preference value will be incremented for a matching route by 555.

Examples

```
-> ip bgp policy route-map routemap1 1 lpref 555
-> ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list	Creates or deletes a policy route map.
ip bgp policy route-map lpref-mode	Configures the action to be taken when setting local preference attribute for a local matching route.

MIB Objects

alaBgpRouteMapTable
 alaBgpRouteMapLocalPref

ip bgp policy route-map lpref-mode

Configures the action to be taken when setting local preference attribute for a local matching route.

ip bgp policy route-map *name sequence_number lpref-mode* {**none** | **inc** | **dec** | **rep**}

Syntax Definitions

name	The route map name.
sequence_number	The route map sequence number. The valid range is 1–255.
none	Do not set the local preference attribute.
inc	Increment the local preference attribute in the matching route by the value specified in the ip bgp policy route-map med command. No action is taken if no local preference attribute is found in the matching route.
dec	Decrement the local preference attribute in the matching route by the value specified in the ip bgp policy route-map med command. No action is taken if no local preference attribute is found in the matching route.
rep	Replace the local preference attribute in the matching route by the value specified in the ip bgp policy route-map med command even if no local preference attribute is found in the matching route.

Defaults

parameter	default
none inc dec rep	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used in conjunction with **ip bgp policy route-map lpref**. The example below shows the combined usage.
- In this example, the local preference value is incremented for a matching route by 555.

Examples

```
-> ip bgp policy route-map routemap1 1 lpref-mode none
-> ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|---|--|
| ip bgp policy prefix6-list | Creates or deletes a policy route map. |
| ip bgp policy route-map lpref | Configures the local preference value for the route map. |
| ip bgp policy route-map med | Configures the Multi-Exit Discriminator (MED) value for a route map. |

MIB Objects

alaBgpRouteMapTable
alaBgpRouteMapLocalPrefMode

ip bgp policy route-map match-community

Configures a matching community primitive for the route map.

ip bgp policy route-map *name sequence_number match-community* [**none** | **no-export** | **no-advertise** | **no-export-subconfed** | *num:num*]

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
none	Removes the community match from the route-map.
no-export	Routes in this community are advertised within the AS but not beyond the local AS.
no-advertise	Routes matching the community restricting advertisement to any peer.
no-export-subconfed	Routes matching the community restricting advertisement to any external BGP peer.
<i>num:num</i>	The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.

Defaults

parameter	default
<i>community_string</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command allows a matching community string primitive to be placed directly in the route map. By default, no community string is specified. The default behavior can be reset by changing the value to “none”.

Examples

```
-> ip bgp policy route-map routemap1 1 match-community 400:1 500 700:1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#) Creates or deletes a policy route map.

MIB Objects

alaBgpRouteMapTable
 alaBgpRouteMapMatchCommunity

ip bgp policy route-map match-mask

Configures a matching mask primitive in the route map.

ip bgp policy route-map *name* *sequence_number* **match-mask** *ip_address*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>ip_address</i>	The 32-bit IP address of the matching mask or “none”.

Defaults

parameter	default
<i>ip_address</i>	0.0.0.0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows a matching mask primitive to be placed directly in the route map. By default, no mask primitive is specified. The default behavior can be reset by changing the value to “**none**”.
- The example on the next line shows usage combined with the [ip bgp policy route-map match-prefix](#) command.

Examples

```
-> ip bgp policy route-map routemap1 1 match-mask 255.255.0.0
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0 match-mask 255.255.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- [ip bgp policy prefix6-list](#) Creates or deletes a policy route map.
- [ip bgp policy route-map match-prefix](#) Configures a matching prefix primitive in the route map.

MIB Objects

alaBgpRouteMapTable
 alaBgpRouteMapMatchMask

ip bgp policy route-map match-prefix

Configures a matching prefix primitive in the route map.

ip bgp policy route-map *name* *sequence_number* **match-prefix** *ip_address*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>ip_address</i>	The 32-bit IP address of the matching prefix.

Defaults

parameter	default
<i>ip_address</i>	0.0.0.0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows a matching prefix primitive to be placed directly in the route map. By default, no prefix primitive is specified. The default behavior can be reset by changing the value to “**none**”.
- The example on the next line shows usage combined with the [ip bgp policy route-map match-mask](#) command.

Examples

```
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0
-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0 match-mask 255.255.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy route-map match-mask](#) Configures a matching prefix primitive in the route map.

[ip bgp policy prefix6-list](#) Configures an AS path matching regular expression primitive in the route map.

MIB Objects

alaBgpRouteMapTable
 alaBgpRouteMapMatchPrefix

ip bgp policy route-map match-regexp

Configures an AS path matching regular expression primitive in the route map.

```
ip bgp policy route-map name sequence_number match-regexp "regular_expression"
```

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>regular_expression</i>	Regular expression or “none”. The regular expression must be enclosed by quotation marks.

Defaults

parameter	default
<i>regular_expression</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows a regular expression matching directive to be placed directly in the route map. By default, no matching regular expression is specified. Regular expressions are defined in [ip bgp policy aspath-list](#) on page 22-96.
- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.
- The default behavior can be reset by changing the value to “**none**”.
- See the *OmniSwitch 10K Advanced Routing Configuration Guide* for more information on the use of regular expressions in BGP commands.

Examples

```
-> ip bgp policy route-map routemap1 1 match-regexp "500 .* 400$"
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#)

Configures an AS path matching regular expression primitive in the route map.

MIB Objects

alaBgpRouteMapTable

alaBgpRouteMapMatchAsRegExp

ip bgp policy route-map med

Configures the Multi-Exit Discriminator (MED) value for a route map.

ip bgp policy route-map *name sequence_number med value*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>value</i>	The MED value. The valid range is 0–4294967295.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command is used in conjunction with [ip bgp policy route-map med-mode](#) command. The first example below shows the combined usage. In the second example, the MED value is incremented for a matching route by 5.

Examples

```
-> ip bgp policy route-map routemap1 1 med 555
-> ip bgp policy route-map routemap1 1 med 555 med-mode inc
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map med-mode	Configures Multi-Exit Discriminator (MED) value for a route map.
ip bgp policy prefix6-list	Configures an AS path matching regular expression primitive in the route map.

MIB Objects

alaBgpRouteMapTable
alaBgpRouteMapMed

ip bgp policy route-map med-mode

Configures the action to be taken when setting the Multi-Exit Discriminator (MED) attribute for a matching route.

ip bgp policy route-map *name sequence_number med-mode* {**none** | **inc** | **dec** | **rep**}

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
none	Do not set the MED.
inc	Increment the MED in the matching route by the value specified in the ip bgp policy route-map med command. No action is taken if no MED is found in the matching route.
dec	Decrement the MED in the matching route by the value specified in the ip bgp policy route-map med command. No action is taken if no MED is found in the matching route.
rep	Replace the MED in the matching route by the value specified in the ip bgp policy route-map med command even if no MED is found in the matching route.

Defaults

parameter	default
none inc dec rep	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command is used in conjunction with **ip bgp policy route-map med**. The first example below shows the combined usage. In the second example, the MED value is incremented for a matching route by 5.

Examples

```
-> ip bgp policy route-map routemap1 1 med-mode inc
-> ip bgp policy route-map routemap1 1 med 5 med-mode inc
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bgp policy route-map med** Configures action to take when setting Multi-Exit Discriminator (MED) attribute for a matching route.
- ip bgp policy prefix6-list** Configures an AS path matching regular expression primitive in the route map.

MIB Objects

alaBgpRouteMapTable
alaBgpRouteMapMedMode

ip bgp policy route-map origin

Configures the action to be taken on the origin attribute when a match is found.

```
ip bgp policy route-map name sequence_number origin {igp | egp | incomplete | none}
```

Syntax Definitions

<i>name</i>	Route map name.
<i>sequence_number</i>	Route map sequence number. Valid range 1–255.
igp	Sets the origin attribute to remote internal BGP (IGP).
egp	Sets the origin attribute to local external BGP (EGP).
incomplete	Sets the origin attribute to incomplete, meaning the origin is unknown.
none	Sets the origin attribute to “none”.

Defaults

parameter	default
igp egp incomplete none	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

By default, no action is taken on the origin attribute when a match is found. The default behavior can be reset by changing the value to “**none**”.

Examples

```
-> ip bgp policy route-map routemap1 1 origin egp
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map origin Configures action to take on origin attribute when a match is found.

ip bgp policy prefix6-list Configures an AS path matching regular expression primitive in the route map.

MIB Objects

alaBgpRouteMapTable

alaBgpRouteMapOrigin

ip bgp policy route-map prefix-list

Assigns a prefix matching list to the route map.

ip bgp policy route-map *name sequence_number prefix-list prefix_name*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>prefix_name</i>	The prefix list name or “none”.

Defaults

parameter	default
<i>prefix_name</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- By default, no prefix list is assigned to the route map. The default behavior can be reset by changing the value to “**none**”.
- The [ip bgp policy prefix-list](#), [ip bgp policy prefix-list action](#), [ip bgp policy prefix-list ge](#), and [ip bgp policy prefix-list le](#) commands are used to create and set permit/deny actions for a prefix path list.

Examples

```
-> ip bgp policy route-map routemap1 1 prefix-list listC
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|---|---|
| ip bgp policy prefix-list | Assigns a prefix matching list to the route map. |
| ip bgp policy prefix-list action | Configures action to be taken for a prefix list when a match is found. |
| ip bgp policy prefix6-list | Configures an AS path matching regular expression primitive in the route map. |

MIB Objects

alaBgpRouteMapTable
 alaBgpRouteMapPrefixMatchListId

ip bgp policy route-map weight

Configures a BGP weight value to be assigned to inbound routes when a match is found.

ip bgp policy route-map *name sequence_number weight value*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>value</i>	The weight value. The valid range is 0–65535.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command sets the weight value for routes that pass the route map match criteria. It is only applicable for the inbound policy. The default value of zero means that the weight is not changed by the route map.

Examples

```
-> ip bgp policy route-map routemap1 1 weight 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#) Configures an AS path matching regular expression primitive in the route map.

MIB Objects

alaBgpRouteMapTable
 alaBgpRouteMapWeight

ip bgp policy route-map community-strip

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

ip bgp policy route-map *name* *sequence_number* **community-strip** *community_list*

Syntax Definitions

<i>name</i>	The route map name.
<i>sequence_number</i>	The route map sequence number. The valid range is 1–255.
<i>community_list</i>	The community list name.

Defaults

No IP BGP policy route-map community list exists.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

Examples

```
-> ip bgp policy route-map routemap1 1 community_strip communitylist
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp policy prefix6-list](#) Configures an AS path matching regular expression primitive in the route map.

MIB Objects

alaBgpRouteMapTable
alaBgpRouteMapCommunityStrip

show ip bgp

Displays the current global settings for the local BGP speaker.

show ip bgp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Most of the parameters in this display can be altered through BGP global commands. See the output definitions below for references to the CLI commands used to configure individual parameters.

Examples

```
-> show ip bgp
Admin Status                = disabled,
Operational Status         = down,
Autonomous system Number   = 1,
BGP Router Id              = 128.0.1.4,
Confederation Id           = 0,
IGP Synchronization Status = disabled,
Minimum AS origin interval (seconds) = 15,
Default Local Preference   = 100,
Route Reflection            = disabled,
Cluster Id                  = 0.0.0.0,
Missing MED Status         = Best,
Aspath Comparison          = enabled,
Always Compare MED         = disabled,
Fast External Fail Over    = disabled,
Log Neighbor Changes       = disabled,
Multi path                  = disabled,
Graceful Restart           = enabled,
Graceful Restart Status    = Not Restarting,
Configured Graceful Restart Interval = 90s,
IPv4 Unicast               = enabled,
IPv6 Unicast               = disabled
```

output definitions

Admin Status	Indicates whether the BGP protocol has been enabled or disabled through the ip bgp admin-state command.
Operational Status	Indicates if the local BGP speaker is actively participating in BGP messages, update, routing advertisements.

output definitions (continued)

Autonomous system Number	The AS assigned to the local BGP speaker through the ip bgp autonomous-system command.
BGP Router Id	The IP address for the local BGP speaker.
Confederation Id	Shows the confederation number assigned to the local BGP speaker. If the BGP speaker does not belong to a confederation, then this value will be zero (0). Confederation numbers are assigned through the ip bgp confederation identifier command.
IGP Synchronization Status	Indicates whether BGP is synchronizing its routing tables with those on non-BGP routers handling IGP traffic (such as a RIP or OSPF router). This value is configured through the ip bgp synchronization command.
Minimum AS origin interval	The frequency, in seconds, at which routes local to the autonomous system are advertised. This value is configured through the ip bgp as-origin-interval command.
Default Local Preference	The local preference that will be assigned to routes that do not already contain a local preference value. This default value is configured through the ip bgp default local-preference command.
Route Reflection	Indicates whether the local BGP speaker is acting as a route reflector for its AS. This value is configured through the ip bgp client-to-client reflection command.
Cluster Id	The IP address for cluster in route reflector configurations using multiple, redundant route reflectors. A value of 0.0.0.0 indicates that a cluster is not set up. This value is configured through the ip bgp cluster-id command.
Missing MED Status	Indicates the MED value that will be assigned to paths that do not contain MED values. Missing MED values will either be assigned to the worst possible value ($2^{32}-1$) or the best possible value (0). This value is set using the ip bgp bestpath med missing-as-worst command. By default, missing MED values are treated as best .
Aspath Comparison	Indicates whether the AS path will be in used in determining the best route. This value is configured through the ip bgp bestpath as-path ignore command.
Always Compare MED	Indicates whether multi-exit discriminator (MED) values are being compared only for internal peers or also for external peers. This value is configured through the ip bgp always-compare-med command.
Fast External Fail Over	Indicates whether Fast External Failover has been enabled or disabled. When enabled a BGP sessions will be reset immediately after a connection to a directly connected external peer goes down. This value is configured through the ip bgp fast-external-failover command.
Log Neighbor Changes	Indicates whether logging of peer state changes is enabled or disabled. This value is configured through the ip bgp log-neighbor-changes command.
Multi path	Indicates whether support for multiple equal cost paths is enabled or disabled. This value is configured through the ip bgp maximum-paths command.
Graceful Restart	Indicates whether graceful restart is enabled or disabled.

output definitions (continued)

Graceful Restart Status	Indicates the graceful restart state. This feature is not supported in Multiprotocol BGP.
Configured Graceful Restart Interval	Indicates the timer for achieving a graceful restart.
IPv4 Unicast	Indicates whether IPv4 unicast is enabled or disabled.
IPv6 Unicast	Indicates whether IPv6 unicast is enabled or disabled.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp unicast	Enables or disables unicast IPv4 updates for the BGP routing process.
ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process
show ip bgp statistics	Displays BGP global statistics.

MIB Objects

```

alabgpMIBGlobalsGroup
  alaBgpProtoStatus
  alaBgpAutonomousSystemNumber
  alaBgpIgpSynchStatus
  alaBgpProtoOperState
  alaBgpNumActiveRoutes
  alaBgpNumEstabExternalPeers
  alaBgpNumEstabInternalPeers
  alaBgpClusterId
  alaBgpDefaultLocalPref
  alaBgpFastExternalFailOver
  alaBgpMedAlways
  alaBgpMissingMed
  alaBgpRouterId
  alaBgpRouteReflection
  alaBgpAsOriginInterval
  alaNumIgpSyncWaitPaths
  alaBgpManualTag
  alaBgpPromiscuousneighbors
  alaBgpConfedId
  alaBgpMultiPath
  alaBgpMaxPeers
  alaBgpPeersChanges

```

show ip bgp statistics

Displays BGP global statistics.

show ip bgp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command show various BGP statistics for the router, such as number of neighbors, active prefixes, number of paths, etc.

Examples

```
-> show ip bgp statistics
# of Active Prefixes Known           = 0,
# of EBGP Neighbors in Established State = 0,
# of IBGP Neighbors in Established State = 0,
# of Feasible Paths                  = 0,
# of Dampened Paths                  = 0,
# of Unsynchronized Paths            = 0,
# of Policy unfeasible paths         = 0,
Total Number of Paths                = 0
```

output definitions

# of Active Prefixes Known	The number of prefixes, or route paths, currently known to the local BGP speaker, that are currently up and active.
# of EBGP Neighbors in Established State	The number of peers outside the AS of the local BGP speaker that the local BGP speaker can route to.
# of IBGP Neighbors in Established State	The number of peers in the same AS as the local BGP speaker that the local BGP speaker can route to.
# of Feasible Paths	The number of route paths that are not active due to one of the following reasons: the route is dampened, the route is not permitted based on BGP policies, or the route is waiting to be synchronized with the IGP protocol.
# of Dampened Paths	The number of route paths that are not active because they have violated dampening parameters.
# of Unsynchronized Paths	The number of route paths that are not active because they are waiting to be synchronized with the IGP routing protocol.

output definitions (continued)

# of Unfeasible Paths	The number of route paths that are not active because they are not permitted based on a configured BGP policy.
Total Number of Paths	The total number of paths known to the speaker, active or not.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bgp](#) Displays the current global settings for the local BGP speaker.

MIB Objects

alaBgpStatsTable

show ip bgp dampening

Displays the BGP route dampening settings.

show ip bgp dampening

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command shows the setting for dampening on the router, assuming it is enabled.

Examples

```
-> show ip bgp dampening
Admin Status           = disabled,
Half life value (seconds) = 300,
Reuse value           = 200
Suppress value        = 300,
Max suppress time (seconds) = 1800,
```

output definitions

Admin Status	Indicates whether route dampening is enabled or disabled. This value is configured through the ip bgp dampening command.
Half life value	The half-life interval, in seconds, after which the penalty value for a reachable route will be reduced by half. This value is configured through the ip bgp dampening command.
Reuse value	The value that the route flapping metric must reach before this route is re-advertised. This value is configured through the ip bgp dampening command.
Suppress value	The number of route withdrawals necessary to begin readvertising a previously suppressed route. This value is configured through the ip bgp dampening command.
Max Suppress time	The maximum time (in seconds) that a route will be suppressed. This value is configured through the ip bgp dampening command.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp dampening](#)

Enables or disables BGP route dampening or the suppression of unstable routes.

MIB Objects

```
alaBgpDampTable  
  alaBgpDampEntry  
  alaBgpDampCeil  
  alaBgpDampCutOff  
  alaBgpDampMaxFlapHistory  
  alaBgpDampReuse  
  alaBgpDampening  
  alaBgpDampeningClear
```

show ip bgp dampening-stats

Displays BGP dampening statistics.

show ip bgp dampening-stats [*ip_address ip_mask*] [*peer_address*]

Syntax Definitions

<i>ip_address</i>	A 32-bit IP address.
<i>ip_mask</i>	A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.
<i>peer_address</i>	A 32-bit IP address of peer (neighbor).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays various statistics on routes that have flapped, and are thus subject to the settings of the dampening feature.

Examples

```
-> show ip bgp dampening-stats
```

Network	Mask	From	Flaps	Duration	FOM
155.132.44.73	255.255.255.255	192.40.4.121	8	00h:00m:35s	175

output definitions

Network	The IP address for the local BGP speaker that is responsible for route dampening in this router.
Mask	The mask for the local BGP speaker that is responsible for route dampening in this router.
From	The IP address for the route that is flapping.
Flaps	The number of times this route has moved from an UP state to a DOWN state or from a DOWN state to an UP state. If the route goes down and then comes back up, then this statistics would count 2 flaps.

output definitions (continued)

Duration	The time since the first route flap occurred. In the above example, this route has flapped 8 times in a 35 second period.
FOM	The Figure Of Merit, or instability metric, for this route. This value increases with each unreachable event. If it reaches the cutoff value (configured in ip bgp dampening), then this route will no longer be advertised.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp dampening](#) Enables and disables route dampening.

show ip bgp path

Displays BGP paths.

show ip bgp path

```
[ip-addr ip_address ip_mask]
[aspath-list aspathlist_name]
[community-list community_list_name]
[prefix-list prefix_name]
[route-map routemap_name]
[cidr-only]
[community community_number]
[neighbor-rcv rcv_peer_address]
[neighbor-adv adv_peer_addr]
[regexp "regular_expression"]
[best]
```

Syntax Definitions

<i>ip_address</i>	A 32-bit IP address of the path.
<i>ip_mask</i>	A 32-bit subnet mask of the path.
<i>aspathlist_name</i>	AS path on which to filter.
<i>community_list_name</i>	Community name on which to filter.
<i>prefix_name</i>	Prefix on which to filter.
<i>routemap_name</i>	Route map on which to filter.
cidr-only	Filter out everything except CIDR routes.
<i>community_number</i>	Community number on which to filter.
<i>rcv_peer_address</i>	Filter all except paths received from this path.
<i>adv_peer_addr</i>	Filter all except paths sent to this path.
<i>regular_expression</i>	Regular expression on which to filter. Regular expressions must be enclosed by quotes. For example, "\$100".
best	Show only the best path.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The basic command displays every path currently in the table. Since the number of paths may run into the thousands, this command provides a number of parameters for displaying a specific path or matching entries for a portion of a path or peer address.

Examples

```
-> show ip bgp path
```

```
Legends: Sta      = Path state
```

```
      >          = best, F = feasible
```

```
      P          = policy changing, U = un-synchronized
```

```
      D          = dampened, N = none
```

```
      Nbr        = Neighbor
```

```
      (O)        = Path Origin (? = incomplete, i = igp, e = egp)
```

```
      degPref    = degree of preference
```

Sta	Network	Mask	Nbr address	Next Hop	(O)	degPref
>	192.40.4.0	255.255.255.0	192.40.4.29	192.40.4.29	i	100
>	192.40.6.0	255.255.255.248	192.40.4.29	192.40.4.29	i	100
>	192.40.6.8	255.255.255.248	192.40.4.29	192.40.4.29	i	100
U	110.100.10.0	255.255.255.0	2001:100:3:4::1	110.100.10.20	?	100
U	110.100.11.0	255.255.255.0	2001:100:3:4::1	110.100.10.20	?	100
U	110.100.12.0	255.255.255.0	2001:100:3:4::1	110.100.10.20	?	100
U	110.100.13.0	255.255.255.0	2001:100:3:4::1	110.100.10.20	?	100
U	110.100.14.0	255.255.255.0	2001:100:3:4::1	110.100.10.20	?	100

output definitions

Sta	Status flag. A greater-than sign (>) indicates this is the best route to the destination.
Network	The IP address for this route path. This is the destination of the route.
Mask	The mask for this route path.
Nbr address	The IP or IPv6 address of the BGP peer that is advertising this path.
Next Hop	The next hop along the route path.
(O)	The origin attribute of this route path. A question mark (?) indicates incomplete, and i indicates IGP, and an e indicates EGP.
degPref	The local preference value assigned to this route path.

```
-> show ip bgp path ip-addr 192.40.6.72 255.255.255.248
```

```
BGP Path parameters
```

```
Path address = 192.40.6.72
```

```
Path mask = 255.255.255.248
```

```
Path protocol = ebgp
```

```
Path peer = 192.40.4.29
```

```
  Path nextHop = 192.40.4.29,
```

```
  Path origin = igp,
```

```
  Path local preference = -1,
```

```
  Path state = active,
```

```
  Path weight = 0,
```

```
  Path preference degree = 100,
```

```
  Path autonomous systems = [nAs=2] : 3 2 ,
```

```
  Path MED = -1,
```



```

Path atomic           = no,
Path AS aggregator   = <none>,
Path IPaddr aggregator = <none>,
Path community       = <none>,
Path unknown attribute = <none>

```

output definitions

Path address	The IP address for route path.
Path mask	The mask for this route path.
Path protocol	The protocol from which this route path was learned. Possible values for this field are as follows: local , static , directhost , rip , ospf , isis , ibgp , ebgp , and other .
Path peer	The IP address of the peer that is advertising this route path.
Path nextHop	The next hop along the route path.
Path origin	The BGP origin attribute. Possible values will be igp , egp , incomplete , and none . The origin attribute is considered during the route decision process.
Path local preference	The local preference value for this route as received in an UPDATE message. A negative value (for example, the -1 in the above display) indicates that the local preference value is missing for this route path.
Path state	Path state indicates the state of the path. The possible states are best , feasible , policy-wait , un-synchronized , dampened , or none . When path state is none , it indicates that there are no paths to this prefix and the route is being purged from the system.
Path weight	The path weight as assigned through inbound and outbound policies.
Path preference degree	The local preference assigned to this route through an inbound or outbound policy, or, if the local preference value is missing, the default local preference (which is assigned through the ip bgp default local-preference).
Path autonomous systems	The AS path for this route. These numbers show the ASs through which the route has traversed with the most recent AS listed first. In the above example, this route began its path in AS 2 and then traveled through AS 3.
Path MED	The multi-exit discriminator (MED) value for this route path. A negative value (for example, the -1 in the above display) indicates that the MED value is missing for this route path.
Path atomic	Indicates whether the ATOMIC-AGGREGATE attribute has been set for this route. When set (this field would read yes), this attribute indicates that an aggregate has caused a loss of information for this route (a less specific route was chosen over a more specific route included in the aggregate).
Path AS aggregator	Part of the AGGREGATOR attribute. This field indicates the AS for the BGP speaker that created the aggregate. A value of <none> indicates this is not an aggregate route.
Path IPaddr aggregator	Part of the AGGREGATOR attribute. This field indicates the IP address for the BGP speaker that created the aggregate. A value of <none> indicates that this is not an aggregate route.

output definitions (continued)

Path community	Indicates the community to which this route path belongs, if applicable. A value of <none> indicates that this route does not belong to a community.
Path unknown attribute	Indicates BGP attributes found in UPDATE messages which the router does not support. For example, multi-protocol attributes are not supported by the router in this release, but it is possible for these attributes to appear in a BGP route.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bgp routes](#) Displays BGP route details.

MIB Objects

alaBgpPathTable
alaBgpPathEntry

show ip bgp routes

Displays BGP route details.

show ip bgp routes [*network_address ip_mask*]

Syntax Definitions

network_address A 32-bit IP address.

ip_mask A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays all the routes in the routing table with details.

Examples

-> show ip bgp routes

Legends: ECL = EBGp change list, ICC = IBGP client change list

ICL = IBGP change list, LCL = local change list

AGG = Aggregation, AGC = Aggregation contribution

AGL = Aggregation list, GDL = Deletion list

AGW = Aggregation waiting, AGH = Aggregation hidden

DMP = Dampening, ACT = Active route

Address	Mask	ECL	ICC	ICL	LCL	AGG	AGC	AGL	AGW	AGH	GDL	DMP	ACT
192.40.4.0	255.255.255.0	No	No	No	No	No	No	No	No	No	No	No	Yes
192.40.6.0	255.255.255.248	No	No	No	No	No	No	No	No	No	No	No	Yes
192.40.6.8	255.255.255.248	No	No	No	No	No	No	No	No	No	No	No	Yes
192.40.6.72	255.255.255.248	No	No	No	No	No	No	No	No	No	No	No	Yes
192.40.6.80	255.255.255.248	No	No	No	No	No	No	No	No	No	No	No	Yes
192.40.6.104	255.255.255.248	No	No	No	No	No	No	No	No	No	No	No	Yes
192.40.6.112	255.255.255.248	No	No	No	No	No	No	No	No	No	No	No	Yes
192.40.6.144	255.255.255.248	No	No	No	No	No	No	No	No	No	No	No	Yes

output definitions

Address	The route destination network address.
Mask	The route destination network mask.
ECL	External BGP change list. When Yes, this route will be advertised as soon as the route advertisement timer expires.
ICC	Internal BGP client change list. When Yes, this route will be advertised to internal non-clients.

output definitions (continued)

ICL	Internal BGP change list. When Yes, this route has changes that need to be advertised.
LCL	Local change list. When Yes, this route is local.
AGG	Aggregation. When Yes, this route is an aggregate route.
AGC	Aggregation contribution. When Yes, this route is part of an aggregate route.
AGL	Aggregation list. When Yes, this route is placed on an aggregate list.
AGW	Aggregation waiting. When Yes, this route is waiting for an aggregate contributor.
AGH	Aggregation hidden. When Yes, this route is hidden as part of an aggregate route.
GDL	Deletion list. When Yes, this route will be deleted.
DMP	Dampening. Indicate whether this route has been dampened. If 'Yes', then this route has been dampened and a dampening history exists.
ACT	Active route. When Yes, the route is active.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bgp path](#) Displays BGP paths.

MIB Objects

alaBgpRouteTable
alaBgpRouteEntry

show ip bgp aggregate-address

Displays aggregate route status.

show ip bgp aggregate-address [*ip_address ip mask*]

Syntax Definitions

ip_address

The 32-bit IP address of the aggregate address.

ip_mask

The 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays a specific aggregate address, or all aggregate addresses on the router.

Examples

```
-> show ip bgp aggregate-address
Network          Mask          Summarize As-Set  Admin state Oper state
-----+-----+-----+-----+-----+-----
155.132.44.73   255.255.255.255 disabled  disabled disabled  not_active
192.40.6.0      255.255.255.255 disabled  disabled disabled  not_active
```

```
-> show ip bgp aggregate-address 192.40.6.0 255.255.255.255
Aggregate address      = 192.40.6.0,
Aggregate mask         = 255.255.255.255,
Aggregate admin state  = disabled,
Aggregate oper state   = not_active,
Aggregate as-set       = disabled,
Aggregate summarize    = disabled,
Aggregate metric       = 0,
Aggregate local preference = 0,
Aggregate community string = 0:500 400:1 300:2
```

output definitions

Network or Aggregate address	The IP address for this aggregate route. This value is configured through the ip bgp aggregate-address command.
Mask or Aggregate mask	The mask for this aggregate route. This value is configured through the ip bgp aggregate-address command.
Summarize or Aggregate summarize	Indicates whether aggregate summarization is enabled or disabled for this aggregate route. This value is configured through the ip bgp aggregate-address summary-only command.

output definitions (continued)

As-Set or Aggregate as-set	Indicates whether AS path aggregate is enabled or disabled. This value is configured through the ip bgp aggregate-address as-set command.
Admin State or Aggregate admin state	Indicates whether this aggregate route is administratively enabled or disabled. This value is configured through the ip bgp aggregate-address admin-state command.
Oper State or Aggregate oper state	Indicates whether this aggregate route is operational and participating in BGP message exchanges.
Aggregate metric	The multi-exit discriminator (MED) value configured for this aggregate route. This value is configured through the ip bgp aggregate-address metric command.
Aggregate local preference	The local preference value for this aggregate route. This value is configured through the ip bgp aggregate-address local-preference command.
Aggregate community string	The community string value for this aggregate route. This value is configured through the ip bgp aggregate-address community command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp aggregate-address Creates and deletes a BGP aggregate route.

MIB Objects

```
alabgpMIBAggrGroup
  alaBgpAggrSet
  alaBgpAggrLocalPref
  alaBgpAggrMetric
  alaBgpAggrSummarize
  alaBgpAggrCommunity
```

show ip bgp network

Displays currently defined network configurations.

show ip bgp network [*network_address ip_mask*]

Syntax Definitions

network_address A 32-bit IP address.

ip_mask A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays all the configured networks, or a single network.

Examples

```
-> show ip bgp network
Network      Mask                Admin state Oper state
-----+-----+-----+-----
155.132.1.2  255.255.255.255 disabled  not_active
155.132.1.3  255.255.255.255 disabled  not_active
```

```
-> show ip bgp network 155.132.1.2 255.255.255.255
Network address      = 155.132.1.2,
Network mask         = 255.255.255.255,
Network admin state  = disabled,
Network oper state   = not_active,
Network metric       = 0,
Network local preference = 0,
Network community string = 0:500 400:1 300:2
```

output definitions

Network or Network address	The IP address configured for this local BGP network. This value is configured through the ip bgp network command.
Mask or Network mask	The mask configured for this local BGP network. This value is configured through the ip bgp network command.
Admin state or Network admin state	Indicates whether this local BGP network is administratively enabled or disabled. This value is configured through the ip bgp network admin-state command.

output definitions (continued)

Oper state or Network oper state	Indicates whether this BGP local network is operationally active or inactive.
Network metric	The multi-exit discriminator (MED) value configured for this local BGP network. This value is configured through the ip bgp network metric command.
Network local preference	The local preference value for this local BGP network. This value is configured through the ip bgp network local-preference command.
Network community string	The community string value for this local BGP network. This value is configured through the ip bgp network community command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network Configures a local BGP network.

MIB Objects

alabgpMIBNetworkGroup

alaBgpNetworkEntry

show ip bgp neighbors

Displays the configured IPv4 BGP peers.

show ip bgp neighbors [*ip_address*]

Syntax Definitions

ip_address A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

There are two output options for this command. If you specify `show ip bgp peer` without a peer IP address, then you see summary information for all peers known to the local BGP speaker. If you enter a specific peer IP address with the command, then you see detailed parameter information for that peer only.

Examples

```
-> show ip bgp neighbors
```

```
Legends:Nbr = Neighbor
```

```
      As = Autonomous System
```

Nbr	address	As	Admin state	Oper state	BgpId	Up/Down
192.40.4.29		3	enabled	estab	192.40.4.29	00h:14m:48s
192.40.4.121		5	disabled	idle	0.0.0.0	00h:00m:00s

output definitions

Nbr address	The IP address for this BGP peer. Assign this address through the ip bgp neighbor command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned through the ip bgp neighbor remote-as command.
Admin state	Indicates whether this peer has been enabled or disabled through the ip bgp neighbor admin-state command.
Oper state	The current BGP state for this peer. Possible states are idle , connect , active , opensent , openconfirm , and established .
BgpId	The unique BGP identifier of the peer. This value is configured through the ip bgp neighbor update-source command.
Up/Down	The time since this peer has transitioned to its current UP or DOWN state. If the peer is currently Established, then this is the time that the peer has been UP. If the peer is currently Idle, then this is the time the peer has been DOWN.

```

-> show ip bgp neighbors 0.0.0.1
Neighbor address                = 0.0.0.1,
Neighbor autonomous system      = 1,
Neighbor Admin state            = enabled,
Neighbor Oper state             = connect,
Neighbor passive status         = disabled,
Neighbor name                   = peer(0.0.0.1),
Neighbor local address          = vlan-215,
Neighbor EBGP multiHop          = enabled,
Neighbor next hop self          = disabled,
Neighbor Route Refresh          = enabled,
Neighbor Ipv4 unicast           = enabled,
Neighbor Ipv4 multicast        = disabled,
Neighbor type                   = internal,
Neighbor auto-restart           = enabled,
Neighbor route-reflector-client = disabled,
Neighbor confederation status  = disabled,
Neighbor remove private AS      = disabled,
Neighbor default originate      = disabled,
Neighbor maximum prefixes       = 5000,
Neighbor max prefixes warning   = enabled,
# of prefixes received          = 0,
Neighbor MD5 key                = <none>,
Neighbor local port             = 0,
Neighbor TCP window size        = 32768
Graceful Restart State          = None,
Advertised Restart Interval     = 0s,
Forwarding State during restart = NotPreserved,
Activate IPv6 unicast           = enabled,
Configured IPv6 NextHop Address = ::,
Neighbor Ipv6 unicast           = advertised

```

output definitions

Neighbor address	The IP address for this BGP peer. Assign this address through the ip bgp neighbor command.
Neighbor autonomous system	The autonomous system to which this peer belongs. A peer's AS number is assigned through the ip bgp neighbor remote-as command.
Neighbor Admin state	Indicates whether this peer has been enabled or disabled through the ip bgp neighbor admin-state command.
Neighbor Oper state	The current BGP state for this peer. Possible states are idle , connect , active , opensent , openconfirm , and established .
Neighbor passive status	Indicates whether the local BGP speaker is "passive" (i.e., waiting for this peer to initiate a session). This value is configured through the ip bgp neighbor passive command.
Neighbor name	The name assigned to this peer through the ip bgp neighbor description command.
Neighbor local address	The interface assigned to this peer. This value is configured through the ip bgp neighbor update-source command.
Neighbor EBGP multihop	Indicates whether BGP multi-hop support is enabled or disabled. This supports allows external BGP peers to communicate with each other even when they are not directly connected. This value is configured through the ip bgp neighbor ebgp-multihop command.

output definitions (continued)

Neighbor next hop self	Indicates whether this peer is using next hop processing. This value is configured through the ip bgp neighbor next-hop-self command.
Neighbor Route Refresh	Indicates whether this peer supports Route Refresh capability as defined in RFC 2918. This capability is an alternative to soft-reconfiguration that can save CPU and memory resources. It allows peers to dynamically request the re-advertisement of BGP routing tables. Since this router supports route refresh all BGP peers are automatically enabled for this capability.
Neighbor Ipv4 unicast	Indicates whether this peer is multi-protocol IP version 4 unicast capable. This router is IPv4 unicasts capable so all peers will be enabled for this capability.
Neighbor Ipv4 multicast	Indicates whether this peer is multi-protocol IP version 4 multicast capable. This router is not IPv4 multicasts capable so all peers will be disabled for this capability.
Neighbor type	Indicates whether this peer is internal or external to the router.
Neighbor auto-restart	Indicates whether peer auto-restart is enabled or disabled. This value is configured through the ip bgp neighbor auto-restart command.
Neighbor route-reflector-client	Indicates whether this peer is a client to the local route reflector, if configured. This value is configured through the ip bgp neighbor route-reflector-client command.
Neighbor confederation status	Indicates whether this peer is a member of a BGP confederation. This value is configured through the ip bgp confederation neighbor command.
Neighbor remove private AS	Indicates whether the stripping of private AS numbers (64512 to 65535) from AS paths is enabled or disabled. This value is configured through the ip bgp neighbor remove-private-as command.
Neighbor default originate	Indicates whether peer default origination is enabled or disabled. When enabled, the local BGP speaker advertises itself as a default to the peer. This value is configured through the ip bgp neighbor default-originate command.
Neighbor maximum prefixes	The maximum number of prefixes the local router can receive in UPDATE from this peer. This value is configured through the ip bgp neighbor maximum-prefix command.
Neighbor max prefixes warning	Indicates whether a warning will be issued when this peer exceeds 80 percent of the maximum prefix value. This value is configured through the ip bgp neighbor update-source command.
# of prefixes received	Displays the total number of prefixes received by this neighbor.
Neighbor MD5 key [32- 47]	When present, shows an encrypted version of the MD5 password. When not present, and MD5 password has not been configured. This value is configured through the ip bgp neighbor md5 key command.
Neighbor local port	The TCP port used for the session with this peer.
Neighbor TCP window size	The size of the TCP window for this BGP session. This value will always be 32768 as that is the maximum size of a BGP message.
Graceful Restart State	Indicates the graceful restart state. This feature is not supported in Multiprotocol BGP.
Advertised Restart Interval	Indicates the restart interval in seconds.

output definitions (continued)

Forwarding State during restart	Indicates whether the peer has preserved the forwarding state during the graceful restart.
Activate IPv6 unicast	Indicates if the IPv6 unicast updates are enabled or not. Options include enabled or disabled .
Configured IPv6 NextHop Address	Specifies the IPv6 nexthop address. This is specified using the ipv6 bgp neighbor ipv6-nexthop command.
Neighbor Ipv6 unicast	Indicates whether Multiprotocol IPv6 Unicast capability is enabled or disabled between the peers.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor Creates or deletes a BGP peer.

MIB Objects

```

alabgpMIBPeerGroup
  alaBgpPeerAddr
  alaBgpPeerAS
  alaBgpPeerPassive
  alaBgpPeerName
  alaBgpPeerMultiHop
  alaBgpPeerMaxPrefix
  alaBgpPeerMaxPrefixWarnOnly
  alaBgpPeerNextHopSelf
  alaBgpPeerSoftReconfig
  alaBgpPeerInSoftReset
  alaBgpPeerIpv4Unicast
  alaBgpPeerIpv4Multicast
  alaBgpPeerRcvdRtRefreshMsgs
  alaBgpPeerSentRtRefreshMsgs
  alaBgpPeerRouteMapOut
  alaBgpPeerRouteMapIn
  alaBgpPeerLocalAddr
  alaBgpPeerLastDownReason
  alaBgpPeerLastDownTime
  alaBgpPeerLastReadTime
  alaBgpPeerRcvdNotifyMsgs
  alaBgpPeerSentNotifyMsgs
  alaBgpPeerLastSentNotifyReason
  alaBgpPeerLastRecvNotifyReason
  alaBgpPeerRcvdPrefixes
  alaBgpPeerDownTransitions
  alaBgpPeerType
  alaBgpPeerAutoReStart
  alaBgpPeerClientStatus
  alaBgpPeerConfedStatus
  alaBgpPeerRemovePrivateAs
  alaBgpPeerClearCounter
  alaBgpPeerTTL

```

alaBgpPeerAspathListOut
alaBgpPeerAspathListIn
alaBgpPeerPrefixListOut
alaBgpPeerPrefixListIn
alaBgpPeerCommunityListOut
alaBgpPeerCommunityListIn
alaBgpPeerRestart
alaBgpPeerDefaultOriginate
alaBgpPeerReconfigureInBound
alaBgpPeerReconfigureOutBound
alaBgpPeerMD5Key
alaBgpPeerMD5KeyEncrypt
alaBgpPeerRowStatus
alaBgpPeerUpTransitions
alaBgpPeerLocalIntfName

show ip bgp neighbors policy

Displays BGP peer policy information.

```
show ip bgp neighbors policy [ip_address]
```

Syntax Definitions

ip_address A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays all of the configured policies for the router, or the policies configured for a specific peer.

Examples

```
-> show ip bgp neighbors policy
Neighbor address = 0.0.0.0,
  Neighbor autonomous system      = 1,
  Neighbor output policy map name = <none>,
  Neighbor input policy map name  = <none>,
  Neighbor output aspath-list name = <none>,
  Neighbor input aspath-list name = <none>,
  Neighbor output prefix-list name = <none>,
  Neighbor input prefix-list name = <none>,
  Neighbor output community-list name = <none>,
  Neighbor input community-list name = <none>,
  Neighbor soft reconfiguration   = enabled
Neighbor address = 0.0.0.1,
  Neighbor autonomous system      = 1,
  Neighbor output policy map name = <none>,
  Neighbor input policy map name  = <none>,
  Neighbor output aspath-list name = <none>,
  Neighbor input aspath-list name = <none>,
  Neighbor output prefix-list name = <none>,
  Neighbor input prefix-list name = <none>,
  Neighbor output community-list name = <none>,
  Neighbor input community-list name = <none>,
  Neighbor soft reconfiguration   = enabled
```

output definitions

Neighbor autonomous system	The AS to which the peer is assigned. This can be assigned by using the ip bgp neighbor remote-as command.
Neighbor output policy map name	The outbound route map policy for the peer. This can be assigned by using the ip bgp neighbor route-map command.
Neighbor input policy map name	The inbound route map policy for the peer. This can be assigned by using the ip bgp neighbor route-map command.
Neighbor output aspath-list name	The outbound AS path list policy for the peer. This can be assigned by using the ip bgp neighbor out-aspathlist command.
Neighbor input aspath-list name	The inbound AS path list policy for the peer. This can be assigned by using the ip bgp neighbor in-aspathlist command.
Neighbor output prefix-list name	The outbound prefix list policy for the peer. This can be assigned by using the ip bgp neighbor out-prefixlist command.
Neighbor input prefix-list name	The inbound prefix list policy for the peer. This can be assigned by using the ip bgp neighbor in-prefixlist command.
Neighbor output community-list name	The outbound community list policy for the peer. This can be assigned by using the ip bgp neighbor out-communitylist command.
Neighbor input community-list name	The inbound community list policy for the peer. This can be assigned by using the ip bgp neighbor in-communitylist command.
Neighbor soft reconfiguration	Lists whether soft reconfigurations are enabled or disabled for this peer. This is configured using the ip bgp neighbor soft-reconfiguration command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp neighbors Displays BGP peer main status.

MIB Objects

N/A

show ip bgp neighbors timer

Displays BGP peer timer statistics.

show ip bgp neighbors timer [*ip_address*]

Syntax Definitions

ip_address A 32-bit IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays the timer values for all peer associated with this speaker, or for a specific peer.

Examples

```
-> show ip bgp neighbors timer
Legends: Nbr      = Neighbor
          As       = Autonomous System
          RtAdv    = Route Advertisement
          Kalive   = Keep Alive (actual)
          Ka(C)    = Configured Keep Alive
```

Nbr	address	As	Hold	Hold(C)	RtAdv	Retry	Kalive	Ka(C)
192.40.4.29		3	90	90	30	120	30	30
192.40.4.121		5	0	90	30	120	0	30

output definitions

Nbr address	The IP address for this BGP peer. Assign this address through the ip bgp neighbor command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned through the ip bgp neighbor remote-as command.
Hold	The current count for the holdtime value.
Hold(C)	The holdtime value configured through the ip bgp neighbor timers command.
RtAdv	The route advertisement interval, in seconds, for updates between external BGP peers. This value is configured through the ip bgp neighbor advertisement-interval command.
Retry	The interval, in seconds, between retries by this peer to set up a connection through TCP with another peer. This value is configured through the ip bgp neighbor timers command.

output definitions (continued)

Kalive	The current count, in seconds, between keepalive messages. Keepalive messages do not contain route or status updates; they serve only to tell other peers that the connection is still live and this peer is reachable.
Ka(C)	The keepalive interval as configured through the ip bgp neighbor timers command.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp neighbors Displays BGP peer main status.

MIB Objects

N/A

show ip bgp neighbors statistics

Displays BGP peer message statistics.

show ip bgp neighbors statistics [*ip_address*]

Syntax Definitions

ip_address A 32-bit IP address of the peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays message statistics for all peers associated with this speaker, or with a specific peer.

Examples

```
-> show ip bgp neighbors statistics
```

```
Legends: RMSGS = number of received messages, SMSGS = number of sent messages
          RUPDS = number of Update messages received,
          SUPDS = number of Update messages sent,
          RNOFY = number of Notify messages received,
          SNOFY = number of Notify messages sent
          RPFXS = number of prefixes received
          UPTNS = number of UP transitions
          DNTNS = number of DOWN transitions
```

Nbr	address	As	RMSGS	SMSGS	RUPDS	SUPDS	RNOFY	SNOFY	RPFXS	UPTNS	DNTNS
192.40.4.29		3	110	123	5	0	0	1	8	2	2
192.40.4.121		5	0	0	0	0	0	0	0	0	0

output definitions

Nbr address	The IP address for this peer. This value is configured through the ip bgp neighbor command.
As	The autonomous system to which this peer belongs. This value is configured through the ip bgp neighbor remote-as command.
RMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.
SMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent by this peer.

output definitions (continued)

RUPDS	The number of route UPDATE messages received by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
SUPDS	The number of route UPDATE messages sent by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
RNOFY	The number of NOTIFY messages received by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
SNOFY	The number of NOTIFY messages sent by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
RPFXS	The number of unique route prefixes received by this peer.
UPTNS	The number of times this peer has come up, operationally.
DNTNS	Number of times this peer has gone down, operationally.

```

-> show ip bgp neighbors statistics 0.0.0.1
Neighbor address                = 0.0.0.1,
# of UP transitions              = 0,
Time of last UP transition      = 00h:00m:00s,
# of DOWN transitions           = 0,
Time of last DOWN transition    = 00h:00m:00s,
Last DOWN reason                = none,
# of msgs rcvd                  = 0,
# of Update msgs rcvd          = 0,
# of prefixes rcvd              = 0,
# of Route Refresh msgs rcvd   = 0,
# of Notification msgs rcvd    = 0,
Last rcvd Notification reason   = none [none]
Time last msg was rcvd         = 00h:00m:00s,
# of msgs sent                  = 0,
# of Update msgs sent           = 0,
# of Route Refresh msgs sent   = 0,
# of Notification msgs sent     = 0,
Last sent Notification reason   = none [none]
Time last msg was sent         = 00h:00m:00s,

```

output definitions

Neighbor address	The IP address for this peer. This value is configured through the ip bgp neighbor command.
# of UP transitions	The number of times this peer has come up, operationally.
Time of last UP transition	The duration that this peer has been up.
# of DOWN transitions	Number of times this peer has gone down, operationally.
Time of last DOWN transition	The duration since this peer last went down.

output definitions (continued)

Last DOWN reason	Provides a message as the last reason why a peer went down. The possible reasons for going down are: user_request - user initiated conn_timeout - connection timer expired hold_timeout - hold timer expired bad_msg - received a bad message from neighbor fsm_blink - BGP FSM error peer_closed - neighbor closed connection peer_notify - neighbor sent fatal notification tcp_error - Fatal TCP error none - None
# of msgs rcvd	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received from this peer.
# of Update msgs rcvd	The number of route UPDATE messages received from this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of prefixes rcvd	The number of unique route prefixes received by this peer.
# of Route Refresh msgs rcvd	The number of route refresh requests this peer has received. Route refresh requests all routes learned by a peer.
# of Notification msgs rcvd	The number of NOTIFY messages received from this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last rcvd Notification reason	<p>NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message received from this peer. The notification reasons are listed in two parts separated by a dash (-). The following are possible notification reasons:</p> <ul style="list-style-type: none"> message header error - synchronization loss message header error - bad length message header error - bad type open message error - unsupported version open message error - bad peer autonomous system open message error - bad peer bgp id open message error - unsupported option open message error - authentication failure open message error - unacceptable hold time open message error - unsupported capability update message error - malformed attribute update message error - unknown attribute update message error - missing wellknown attribute update message error - attribute flags error update message error - attribute length error update message error - invalid origin update message error - as loop update message error - invalid nexthop update message error - optional attribute error update message error - invalid network update message error - malformed aspath cease - maximum number of prefixes reached cease - administrative shutdown cease - peer de-configured cease- administrative reset cease- connection rejected cease - other configuration change cease - connection collision resolution cease - out of resources hold time out - none fsm error - none none - none
Time last msg was rcvd	The duration since a message was received from this peer.
# of msgs sent	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent to this peer.
# of Update msgs sent	The number of route UPDATE messages sent to this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of Route Refresh msgs sent	The number of route refresh requests this peer has sent. Route refresh requests request all routes learned be a peer.
# of Notification msgs sent	The number of NOTIFY messages sent to this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last sent Notification reason	NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message sent by this peer. The notification reasons are listed in two parts separated by a dash (-). See the list of possible notification reasons under the description for the Peer last received notification reason field above.
Time last msg was sent	The duration since a message was sent to this peer.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip bgp neighbor](#) Creates or deletes a BGP peer.

MIB Objects

N/A

show ip bgp policy aspath-list

Displays AS path list parameters.

```
show ip bgp policy aspath-list [name] ["regular_expression"]
```

Syntax Definitions

<i>name</i>	An AS path name.
<i>regular_expression</i>	A regular expression. The regular expression must be enclosed by quotation marks.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command displays a list of all of the AS path policies for the router, or a single policy selected by the list name or regular expression.
- Regular expressions are defined in the [ip bgp policy aspath-list](#) command on page 22-96.
- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.

Examples

```
-> show ip bgp policy aspath-list
Aspath List Name      Aspath regular expression
-----+-----
aspl1                  (500 | 400) ? 300$
aspl2                  (500 | 400)
```

```
-> show ip bgp policy aspath-list aspl1
Aspath List name = aspl1
Aspath Regexp    = (500 | 400) ? 300$
  Admin state    = disabled,
  Priority       = 1,
  Action         = deny,
  Primary index  = 0,
```

output definitions

Aspath List name	The name of the AS path list. This is defined using the ip bgp policy aspath-list command.
Aspath regular expression	The regular expression that defines the AS path list. This is defined using the ip bgp policy aspath-list command.

output definitions (continued)

Admin state	The administration state of the AS path policy. It is either enable or disable.
Priority	The AS path list priority. This is defined using the ip bgp policy aspath-list priority command.
Action	The AS path list action, either permit or deny. This is defined using the ip bgp policy aspath-list action command.
Primary index	The instance identifier for the AS path list. This value is not configurable.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy aspath-list Creates or removes an AS path list.

MIB Objects

```
alabgpMIBAspathListGroup
  alaBgpAspathMatchListId
  alaBgpAspathMatchListRegExp
  alaBgpAspathMatchListPriority
  alaBgpAspathMatchListAction
  alaBgpAspathMatchListRowStatus
```

show ip bgp policy community-list

Displays community list parameters.

show ip bgp policy community-list [*name*] [*string*]

Syntax Definitions

name Community name.

string Community match list string

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays a list of the community policies for the speaker, or a specific policy defined by its name or community match string.

Examples

```
-> show ip bgp policy community-list
Community list name      Community string
-----+-----
adfasdf                  0:0
```

```
-> show ip bgp policy community-list com11
Community List name = com11
Community string    = 600:1
  Admin state       = disabled,
  Match type        = exact,
  Priority           = 1,
  Action            = deny,
  Primary index     = 0
```

output definitions

Community List name	The community list name. This is defined using the ip bgp policy community-list command.
Community string	The community list definition. This is defined using the ip bgp policy community-list command.
Admin state	The administration state of the community list policy, either enabled or disabled.
Match type	The match type of the community list. This is defined using the ip bgp policy community-list match-type command.

output definitions (continued)

Priority	The community list priority. This is defined using the ip bgp policy community-list priority command.
Action	The community list action. This is defined using the ip bgp policy community-list action command.
Primary index	The instance identifier for the community list. This value is not configurable.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy community-list Creates or deletes a community list.

MIB Objects

```
alabgpMIBCommunityListGroup
  alaBgpCommunityMatchListId
  alaBgpCommunityMatchListString
  alaBgpCommunityMatchListPriority
  alaBgpCommunityMatchListType
  alaBgpCommunityMatchListAction
  alaBgpCommunityMatchListRowStatus
```

show ip bgp policy prefix-list

Displays prefix list parameters.

```
show ip bgp policy prefix-list [name] [ip_address ip_mask]
```

Syntax Definitions

<i>name</i>	A prefix list name.
<i>ip_address</i>	A prefix list IP address.
<i>ip_mask</i>	An IP address mask.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays the list of prefix-list policies configured for the speaker, or a specific list determined by the list name or IP address and mask.

Examples

```
-> show ip bgp policy prefix-list
Prefix List name      Prefix address  Prefix mask
-----+-----+-----
pfxl1                 155.132.33.0   255.255.255.0
pfxl2                 155.148.32.0   255.255.255.0
```

```
-> show ip bgp policy prefix-list pfxl1
Prefix List name = pfxl1
Address          = 155.132.33.0
Mask            = 255.255.255.0
  Admin state    = disabled,
  Match Mask >= (GE) = 0,
  Match Mask <= (LE) = 0,
  Action        = deny
```

output definitions

Prefix List name	The name of the prefix list. This is defined using the ip bgp policy prefix-list command.
Address	The IP address of the prefix list. This is defined using the ip bgp policy prefix-list command.
Mask	The mask of the prefix list. This is defined using the ip bgp policy prefix-list command.
Admin state	The administrative state of the prefix list, either enabled or disabled.

output definitions (continued)

Match Mask >= (GE)	The GE match mask of the prefix list. This is defined using the ip bgp policy prefix-list ge command.
Match Mask <= (LE)	The LE match mask of the prefix list. This is defined using the ip bgp policy prefix-list le command.
Action	The action of the prefix list. This is defined using the ip bgp policy prefix-list action command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix-list Creates or deletes a prefix match list.

MIB Objects

```
alabgpMIBPrefixListGroup
  alaBgpPrefixMatchListId
  alaBgpPrefixMatchListAddr
  alaBgpPrefixMatchListMask
  alaBgpPrefixMatchListGE
  alaBgpPrefixMatchListLE
  alaBgpPrefixMatchListAction
  alaBgpPrefixMatchListRowStatus
```

show ip bgp policy route-map

Displays policy route map parameters.

show ip bgp policy route-map [*name*] [*sequence_number*]

Syntax Definitions

<i>name</i>	Route map name.
<i>sequence_number</i>	A sequence number. The valid range is 1–255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The route map is displayed as a summary table by entering only the route map name, or as a detailed list by specifying the sequence number.

Examples

```
-> show ip bgp policy route-map
RouteMap name          Instance
-----+-----
rmap1                  1
rmap1                  2
rmap2                  1
```

```
-> show ip bgp policy route-map rmap1
RouteMap name          = rmap1
RouteMap instance     = 1
  Admin state          = disabled,
  Local pref (mode/value) = <none> / 0,
  Route map action     = permit,
  Origin               = <none>,
  MED (mode/value)    = <none> / 0,
  Weight              = 0,
  Aspath-List name     = aspl1,
  Aspath prepend       = <none>,
  Aspath match primitive = 500 .* 400$,
  Prefix-List name     = <none>,
  Prefix match primitive = 0.0.0.0 0.0.0.0,
  Community-List name  = coml2,
  Community match primitive = <none>,
  Community string [mode] = [Additive]
```

output definitions

RouteMap name	The name of the route map policy. This is determined using the ip bgp policy prefix6-list command.
RouteMap instance	The instance of the route map policy. This is determined using the ip bgp policy prefix6-list command.
Admin state	The administrative state of the route map policy, either enabled or disabled.
Local pref (mode/value)	The local preference of the route map policy. This is determined using the ip bgp policy route-map lpref command.
Route map action	The action of the route map policy. This is determined using the ip bgp policy route-map action command.
Origin	The origin of the route map policy. This is determined using the ip bgp policy route-map origin command.
MED (mode/value)	The MED of the route map policy. This is determined using the ip bgp policy route-map med command.
Weight	The weight of the route map policy. This is determined using the ip bgp policy route-map weight command.
Aspath-List name	The name of the AS path list attached to this route map. This is set using the show ip bgp policy aspath-list command.
Aspath prepend	The value to prepend to the AS_PATH attribute of the routes matched by this RouteMap instance (Empty quotes indicates no AS_PATH prepending is to be done).
Aspath match primitive	The regular expression used to match AS Path for this route map.
Prefix-List name	The name of the prefix list attached to this route map. This is set using the show ip bgp policy prefix-list command.
Prefix match primitive	The prefix to match for this route map.
Community-List name	The name of the community list attached to this route map. This is set using the show ip bgp policy community-list command.
Community match primitive	The community string to match for this route map.
Community string [mode]	The name of the community mode attached to this route map. This is set using the ip bgp policy route-map community-mode command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy prefix6-list Creates or deletes a policy route map.

MIB Objects

```
alabgpMIBRouteMapGroup  
  alaBgpRouteMapName  
  alaBgpRouteMapInst  
  alaBgpRouteMapAsPathMatchListId  
  alaBgpRouteMapPrefixMatchListId  
  alaBgpRouteMapCommunityMatchListId  
  alaBgpRouteMapOrigin  
  alaBgpRouteMapLocalPref  
  alaBgpRouteMapLocalPrefMode  
  alaBgpRouteMapMed  
  alaBgpRouteMapMedMode  
  alaBgpRouteMapAsPrepend  
  alaBgpRouteMapSetCommunityMode  
  alaBgpRouteMapCommunity  
  alaBgpRouteMapMatchAsRegExp  
  alaBgpRouteMapMatchPrefix  
  alaBgpRouteMapMatchMask  
  alaBgpRouteMapMatchCommunity  
  alaBgpRouteMapWeight  
  alaBgpRouteMapAction  
  alaBgpRouteMapRowStatus
```

ip bgp graceful-restart

Configures support for the graceful restart feature on a BGP router.

ip bgp graceful-restart

no ip bgp graceful-restart

Syntax Definitions

N/A

Defaults

Graceful restart is enabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable support for the graceful restart feature on a BGP router. It has only unplanned graceful restart.
- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on an OmniSwitch 10K with a single CMM.
- Note that graceful restart does not support IPv6 prefixes at this time.

Examples

```
-> ip bgp graceful restart  
-> no ip bgp graceful restart
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal  
  alaBgpGracefulRestart  
  alaBgpRestartInterval
```

ip bgp graceful-restart restart-interval

Configures the grace period for achieving a graceful BGP restart.

ip bgp graceful-restart restart-interval [*seconds*]

Syntax Definitions

seconds The hitless restart timeout interval, in seconds. The valid range is 1–3600.

Defaults

parameter	default
<i>seconds</i>	90

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The minimum hardware configuration for this command is a redundant CMM configuration. This command is not supported on an OmniSwitch 10K with a single CMM.
- Note that graceful restart does not support IPv6 prefixes at this time.

Examples

```
-> ip bgp graceful-restart restart-interval 600
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bgp](#) Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal
  alaBgpGracefulRestart
  alaBgpRestartInterval
```

ip bgp unicast

Enables or disables unicast IPv4 advertisements for the BGP routing process.

ip bgp unicast

no ip bgp unicast

Syntax Definitions

N/A

Defaults

By default, BGP IPv4 advertisements are enabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to turn off IPv4 unicast advertisements.
- BGP should be disabled before enabling or disabling IPv4 unicast advertisements.
- IPv4 unicast advertisements may be turned off on homogenous IPv6 networks that are not aware of IPv4 routing. In such cases, the command, **ip router router-id**, must be used to explicitly configure the 32-bit unique router identifier.

Examples

```
-> ip bgp unicast
-> no ip bgp unicast
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp unicast	Enables or disables unicast IPv6 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.
ip router router-id	Configures the router ID for the router.

MIB Objects

```
alaBgpGlobal
  alaBgpMultiProtocolIpv4
```

ipv6 bgp unicast

Enables or disables unicast IPv6 advertisements for the BGP routing process.

ipv6 bgp unicast

no ipv6 bgp unicast

Syntax Definitions

N/A

Defaults

By default, IPv6 BGP advertisements are disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to turn off IPv6 unicast advertisements.
- BGP should be disabled before enabling or disabling IPv6 unicast advertisements.

Examples

```
-> ipv6 bgp unicast  
-> no ipv6 bgp unicast
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp unicast	Enables or disables unicast IPv4 updates for the BGP routing process.
show ip bgp	Displays the current global settings for the local BGP speaker.

MIB Objects

```
alaBgpGlobal  
  alaBgpMultiProtocolIpv6
```

ip bgp neighbor activate-ipv6

Enables or disables the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv4 addresses.

ip bgp neighbor *ip_address* **activate-ipv6**

no ip bgp neighbor *ip_address* **activate-ipv6**

Syntax Definitions

ip_address The 32-bit IPv4 address of the neighbor.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to disable the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv4 addresses.

Examples

```
-> ip bgp neighbor 1.0.0.1 activate-ipv6
-> no ip bgp neighbor 1.0.0.1 activate-ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bgp neighbors](#) Displays BGP peer main status.

MIB Objects

```
alaBgpPeerTable
  alaBgpPeerAddr
  alaBgpPeerIpv6Unicast
```

ip bgp neighbor ipv6-nexthop

Configures the IPv6 next hop addresses for the IPv6 prefixes advertised between BGP peers. These BGP peers are identified by their IPv4 addresses.

ip bgp neighbor *ip_address* **ipv6-nexthop** *ipv6_address*

Syntax Definitions

<i>ip_address</i>	The 32-bit IPv4 address of the neighbor.
<i>ipv6_address</i>	A 128-bit global IPv6 address to be used as the next hop for IPv6 routes being advertised to this BGP speaker.

Defaults

By default, the IPv6 next hop value is set to all zeros.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- To reset the IPv6 next hop value, enter an all-zero address.
- For internal BGP (IBGP) peers, the IPv6 next hop is used only if the peer **next-hop-self** option is configured.
- For external BGP (EBGP) peers, the IPv6 next hop is used for all the advertised IPv6 routes.

Examples

```
-> ip bgp neighbor 1.0.0.1 ipv6-nexthop 2001:100:3:4::1
-> ip bgp neighbor 1.0.0.1 ipv6-nexthop ::
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeerTable
  alaBgpPeerAddr
  alaBgpPeerIpv6NextHop
```

show ipv6 bgp path

Displays the known IPv6 BGP paths for all the routes or a specific route.

show ipv6 bgp path [**ipv6-addr** *ipv6_address/prefix_length*]

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

By default, IPv6 BGP paths for all the routes will be displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *ipv6_address/prefix_length* parameter to display the IPv6 BGP paths for a specified route.

Examples

```
-> show ipv6 bgp path
Legends: Sta      = Path state
          >       = best, F = feasible, S = stale
          U       = un-synchronized
          Nbr     = Neighbor
          (O)     = Path Origin (? = incomplete, i = igp, e = egp)
          degPref = degree of preference
```

Sta	Prefix	Nbr	Address	(O)	degPref
>	2020:100:200:1::/64		2001:100:3:4::1	i	100
>	2020:100:200:2::/64		2001:100:3:4::1	i	100
>	2020:100:200:3::/64		2001:100:3:4::1	i	100
>	2020:100:200:4::/64		2001:100:3:4::1	i	100
>	2020:100:200:5::/64		2001:100:3:4::1	i	100
>	2525:2525:1::/48		100.3.4.1	i	100
>	2525:2525:2::/48		100.3.4.1	i	100
>	2525:2525:3::/48		100.3.4.1	i	100
>	2525:2525:4::/48		100.3.4.1	i	100
>	2525:2525:5::/48		100.3.4.1	i	100

output definitions

Sta	Status flag. A greater-than sign (>) indicates this is the best route to the destination.
Prefix	The destination address of the IPv6 route in the hexadecimal format.

output definitions (continued)

Nbr Address	The IP or IPv6 address of the BGP peer that advertises this path.
(0)	The origin attribute of this route path. A question mark (?) indicates incomplete, and i indicates IGP, and an e indicates EGP.
degPref	The local preference value assigned to this route path.

```
-> show ipv6 bgp path ipv6-addr 2020:100:200:1::/64
```

```
BGP Path parameters
```

```
Path address      = 2020:100:200:1::
Path Length      = 64
Path protocol    = ibgp
Path neighbor    = peer(2001:100:3:4::1)
  Path nextHop    = 2001:100:3:4::1,
  Path origin     = igp,
  Path local preference = 100,
  Path state     = active,
  Path weight    = 0,
  Path preference degree = 100,
  Path autonomous systems = [nAs=0] : <none>,
  Path MED       = <none>,
  Path atomic    = no,
  Path AS aggregator = <none>,
  Path IPaddr aggregator = <none>,
  Path community = <none>,
  Path Originator Id = <none>,
  Path Cluster List = <none>,
  Path unknown attribute = <none>
```

output definitions

Path address	The IPv6 address for route path.
Path Length	The prefix length of the IPv6 path.
Path protocol	The protocol from which this route path was learned. Possible values for this field are as follows: local , static , directhost , rip , ospf , isis , ibgp , ebgp , and other .
Path neighbor	The IPv6 address of the BGP peer.
Path nextHop	The next hop along the route path.
Path origin	The BGP origin attribute. Possible values will be igp , egp , incomplete , and none . The origin attribute is considered during the route decision process.
Path local preference	The local preference value for this route as received in an UPDATE message. A negative value (for example, the -1 in the above display) indicates that the local preference value is missing for this route path.
Path state	Indicates the state of the path. The possible states are best , feasible , policy-wait , un-synchronized , dampened , or none . When path state is none , it indicates that there are no paths to this prefix and the route is being purged from the system.
Path weight	The path weight as assigned through inbound and outbound policies.

output definitions (continued)

Path preference degree	The local preference assigned to this route through an inbound or outbound policy, or, if the local preference value is missing, the default local preference (which is assigned through the ip bgp default local-preference).
Path autonomous systems	The AS path for this route. These numbers show the ASs through which the route has traversed with the most recent AS listed first. In the above example, this route began its path in AS 2 and then traveled through AS 3.
Path MED	The multi-exit discriminator (MED) value for this route path. A negative value (for example, the -1 in the above display) indicates that the MED value is missing for this route path.
Path atomic	Indicates whether the ATOMIC-AGGREGATE attribute has been set for this route. When set (this field would read yes), this attribute indicates that an aggregate has caused a loss of information for this route (a less specific route was chosen over a more specific route included in the aggregate).
Path AS aggregator	Part of the AGGREGATOR attribute. This field indicates the AS for the BGP speaker that created the aggregate. A value of <none> indicates this is not an aggregate route.
Path IPaddr aggregator	Part of the AGGREGATOR attribute. This field indicates the IP address for the BGP speaker that created the aggregate. A value of <none> indicates that this is not an aggregate route.
Path community	Indicates the community to which this route path belongs, if applicable. A value of <none> indicates that this route does not belong to a community.
Path Originator Id	The Router Id of the BGP4 speaker that performed route reflection
Path Cluster List	Sequence of Cluster Id values representing the reflection path that the route has passed, if this is a reflected route in the local AS.
Path unknown attribute	Indicates BGP attributes found in UPDATE messages which the router does not support. For example, multi-protocol attributes are not supported by the router in this release, but it is possible for these attributes to appear in a BGP route.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp routes Displays the known IPv6 BGP routes.

MIB Objects

```
alaBgpPath6Table  
  alaBgpPath6Addr  
  alaBgpPath6MaskLen  
  alaBgpPath6PeerBgpId  
  alaBgpPath6SrcProto  
  alaBgpPath6Weight  
  alaBgpPath6Pref  
  alaBgpPath6State  
  alaBgpPath6Origin  
  alaBgpPath6NextHop  
  alaBgpPath6As  
  alaBgpPath6LocalPref  
  alaBgpPath6Med  
  alaBgpPath6Atomic  
  alaBgpPath6AggregatorAs  
  alaBgpPath6AggregatorAddr  
  alaBgpPath6Community  
  alaBgpPath6OriginatorId  
  alaBgpPath6ClusterList  
  alaBgpPath6PeerName  
  alaBgpPath6UnknownAttr
```

show ipv6 bgp routes

Displays the known IPv6 BGP routes.

show ipv6 bgp routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 bgp routes
```

```
Legends: ECL = EBGP change list, ICC = IBGP client change list
          ICL = IBGP change list, LCL = local change list
          AGG = Aggregation, AGC = Aggregation contribution
          AGL = Aggregation list, GDL = Deletion list
          AGW = Aggregation waiting, AGH = Aggregation hidden
          DMP = Dampening, ACT = Active route
```

Prefix	ECL	ICC	ICL	LCL	AGG	AGC	AGL	AGW	AGH	GDL	DMP	ACT
2020:100:200:1::/64	No	No	No	No	No	No	No	No	No	No	No	Yes
2020:100:200:2::/64	No	No	No	No	No	No	No	No	No	No	No	Yes
2020:100:200:3::/64	No	No	No	No	No	No	No	No	No	No	No	Yes
2020:100:200:4::/64	No	No	No	No	No	No	No	No	No	No	No	Yes
2020:100:200:5::/64	No	No	No	No	No	No	No	No	No	No	No	Yes
2525:2525:1::/48	No	No	No	No	No	No	No	No	No	No	No	Yes
2525:2525:2::/48	No	No	No	No	No	No	No	No	No	No	No	Yes
2525:2525:3::/48	No	No	No	No	No	No	No	No	No	No	No	Yes
2525:2525:4::/48	No	No	No	No	No	No	No	No	No	No	No	Yes
2525:2525:5::/48	No	No	No	No	No	No	No	No	No	No	No	Yes

output definitions

Prefix	The destination address of the IPv6 route in the hexadecimal format.
ECL	External BGP change list. When Yes, this route will be advertised as soon as the route advertisement timer expires.
ICC	Internal BGP client change list. When Yes, this route will be advertised to internal non-clients.

output definitions (continued)

ICL	Internal BGP change list. When Yes, this route has changes that need to be advertised.
LCL	Local change list. When Yes, this route is local.
AGG	Aggregation. When Yes, this route is an aggregate route.
AGC	Aggregation contribution. When Yes, this route is part of an aggregate route.
AGL	Aggregation list. When Yes, this route is placed on an aggregate list.
AGW	Aggregation waiting. When Yes, this route is waiting for an aggregate contributor.
AGH	Aggregation hidden. When Yes, this route is hidden as part of an aggregate route.
GDL	Deletion list. When Yes, this route will be deleted.
DMP	Dampening. Indicate whether this route has been dampened. If 'Yes', then this route has been dampened and a dampening history exists.
ACT	Active route. When Yes, the route is active.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp path Displays the known IPv6 BGP paths for all the routes or a specific route.

MIB Objects

```

alaBgpRoute6Table
  alaBgpRoute6Addr
  alaBgpRoute6MaskLen
  alaBgpRoute6State
  alaBgpRoute6IsHidden
  alaBgpRoute6IsAggregate
  alaBgpRoute6IsAggregateContributor
  alaBgpRoute6IsAggregateList
  alaBgpRoute6IsAggregateWait
  alaBgpRoute6IsOnEbgpChgList
  alaBgpRoute6IsOnIbgpClientChgList
  alaBgpRoute6IsOnIbgpChgList
  alaBgpRoute6IsOnLocalChgList
  alaBgpRoute6IsOnDeleteList
  alaBgpRoute6IsDampened

```

ipv6 bgp network

Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

ipv6 bgp network *ipv6_address/prefix_length*

no ipv6 bgp network *ipv6_address/prefix_length*

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to turn off the advertisement of locally reachable IPv6 networks.

Examples

```
-> ipv6 bgp network 2001::1/64
-> no ipv6 bgp network 2001::1/64
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- ipv6 bgp network admin-state** Enables or disables a BGP network.
- show ipv6 bgp network** Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

MIB Objects

```
alaBgpNetwork6Table
  alaBgpNetwork6Addr
  alaBgpNetwork6MaskLen
```

ipv6 bgp network community

Defines a community for a route created by the **ipv6 bgp network** command. Communities are a way of grouping BGP peers that do not share an IPv6 subnet or an AS.

```
ipv6 bgp network ipv6_address/prefix_length [community {none | num | num:num}]
```

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask) (3..128).
none	Removes a prefix from a community.
<i>num</i>	The community attribute number.
<i>num:num</i>	Community attribute in the AA : NN format. AA indicates the autonomous system and NN indicates the community number.

Defaults

By default, a route is not assigned to a community.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **community** attribute is defined.

Examples

```
-> ipv6 bgp network 2004::2/64 community 23:20
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table  
  alaBgpNetwork6Addr  
  alaBgpNetwork6MaskLen  
  alaBgpNetwork6Community
```

ipv6 bgp network local-preference

Defines the local preference value for a route generated by the **ipv6 bgp network** command. This value will override the default local preference value; it is used when announcing this network to internal peers.

ipv6 bgp network *ipv6_address/prefix_length* [**local-preference num**]

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask) (3..128).
<i>num</i>	The local preference attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
<i>num</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **local-preference** attribute is defined.

Examples

```
-> ipv6 bgp network 2004::1/24 local-preference 6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table  
  alaBgpNetwork6Addr  
  alaBgpNetwork6MaskLen  
  alaBgpNetwork6LocalPref
```

ipv6 bgp network metric

Configures the Multi-Exit Discriminator (MED) attribute value for an network generated by the **ipv6 bgp network** command. This value is sent from routers of one AS to another to indicate the path that the remote AS can use to send data to the local AS.

```
ipv6 bgp network ipv6_address/prefix_length [metric num]
```

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask) (3..128).
<i>num</i>	The MED attribute value. The valid range is 0–4294967295.

Defaults

parameter	default
<i>num</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **metric** attribute is defined for the same route.

Examples

```
-> ipv6 bgp network 2001::1/64 metric 20
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp network	Advertises a locally reachable IPv6 address as a IPv6 BGP network to other BGP peers.
show ipv6 bgp network	Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

```
alaBgpNetwork6Table  
  alaBgpNetwork6Addr  
  alaBgpNetwork6MaskLen  
  alaBgpNetwork6Metric
```

ipv6 bgp network admin-state

Enables or disables a BGP network. The BGP status must be manually enabled after configuring all the BGP neighbor and network parameters.

ipv6 bgp network *ipv6_address/prefix_length* [**admin-state** {**enable** | **disable**}]

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask) (3..128).
admin-state	< TBD from updated SFS >.
enable	Enables the BGP network.
disable	Disables the BGP network.

Defaults

By default, the BGP network is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The IPv6 BGP route created with the **ipv6 bgp network** command should exist before the **status** attribute is defined.

Examples

```
-> ipv6 bgp network 2001::1/64 admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp network Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

MIB Objects

alaBgpNetwork6Table
 alaBgpNetwork6Addr
 alaBgpNetwork6MaskLen
 alaBgpNetwork6RowStatus

show ipv6 bgp network

Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

show ipv6 bgp network [*ipv6_address/prefix_length*]

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address.
<i>/prefix_length</i>	The number of bits that are significant in the IPv6 address (mask) (3..128).

Defaults

By default, all IPv6 BGP networks and their status will be displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *ipv6_address/prefix_length* parameter to display the status of a specific IPv6 BGP network.

Examples

```
show ipv6 bgp network
Network                               Admin state Oper state
-----+-----+-----
2525:500:600::/64                    enabled     active
```

```
show ipv6 bgp network 2525:500:600::/64
Network address      = 2525:500:600::/64,
Network admin state  = enabled,
Network oper state   = active,
Network metric       = 0,
Network local preference = 0,
Network community string = <none>
```

output definitions

Network or Network address	The IPv6 address configured for this local BGP network. This value is configured through the ipv6 bgp network command.
Admin state or Network admin state	Indicates whether this local BGP network is administratively enabled or disabled. This value is configured through the ipv6 bgp network admin-state command.
Oper state or Network oper state	Indicates whether this BGP local network is operationally active or inactive.

output definitions (continued)

Network metric	The multi-exit discriminator (MED) value configured for this local BGP network. This value is configured through the ipv6 bgp network metric command.
Network local preference	The local preference value for this local BGP network. This value is configured through the ipv6 bgp network local-preference command.
Network community string	The community string value for this local BGP network. This value is configured through the ipv6 bgp network community command.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp network .Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

MIB Objects

```
alaBgpNetwork6Table
  alaBgpNetwork6Addr
  alaBgpNetwork6MaskLen
  alaBgpNetwork6State
  alaBgpNetwork6Metric
  alaBgpNetwork6LocalPref
  alaBgpNetwork6Community
  alaBgpNetwork6RowStatus
```

ipv6 bgp neighbor

Creates or deletes a BGP peer relationship using IPv6 addresses.

ipv6 bgp neighbor *ipv6_address*

no ipv6 bgp neighbor *ipv6_address*

Syntax Definitions

ipv6_address The 128-bit IPv6 address of the new BGP peer.

Defaults

By default, no BGP peers are configured in the BGP network.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a BGP peer.
- To establish a BGP session, the BGP peer should be reachable.
- You must manually enable a BGP peer after creating it. A BGP peer is enabled using the **ipv6 bgp neighbor admin-state** command.
- Once created, a BGP peer must be assigned an autonomous system number using the **ipv6 bgp neighbor remote-as** command.
- Use **update-source** keyword to configure the IPv6 interface when link-local address is used as neighbor address.

Examples

```
-> ipv6 bgp neighbor 2001::1  
-> no ipv6 bgp neighbor 2001::1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp neighbor admin-state Enables or disables the BGP peer status.

ipv6 bgp neighbor remote-as Assigns an AS number to the BGP peer.

MIB Objects

alaBgpPeer6Table

alaBgpPeer6Addr

ipv6 bgp neighbor activate-ipv6

Enables the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv6 addresses.

ipv6 bgp neighbor *ipv6_address* [**activate-ipv6**]

no ipv6 bgp neighbor *ipv6_address* [**activate-ipv6**]

Syntax Definitions

ipv6_address The 128-bit IPv6 address.

Defaults

This command is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to disable the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv6 addresses.

Examples

```
-> ipv6 bgp neighbor 1.0.0.1 activate-ipv6
-> no ipv6 bgp neighbor 1.0.0.1 activate-ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 bgp neighbors](#) Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
  alaBgpPeer6Addr
  alaBgpPeer6ActivateIpv6
```

ipv6 bgp neighbor ipv6-nexthop

Configures the IPv6 next hop addresses for IPv6 prefixes advertised between BGP peers. These BGP peers are identified by their IPv6 addresses.

```
ipv6 bgp neighbor ipv6_address [ipv6-nexthop ipv6_address]
```

Syntax Definitions

ipv6_address The 128-bit IPv6 address of the next hop router.

Defaults

By default, the IPv6 next hop address is set to all zeros.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- To reset the IPv6 next hop value, enter an all-zero address.
- For internal BGP (IBGP) peers, the IPv6 next hop is used only if the peer **next-hop-self** option is configured.
- For external BGP (EBGP) peers, the IPv6 next hop is used for all the advertised IPv6 routes.
- For BGP peers configured with their link-local addresses, the configured IPv6 next hop is used while advertising IPv6 prefixes.

Examples

```
-> ipv6 bgp neighbor 2001::1 ipv6-nexthop fe80::/24  
-> no ipv6 bgp neighbor 2001::1 ipv6-nexthop fe80::/24
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 bgp neighbors](#) Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table  
  alaBgpPeer6Addr  
  alaBgpPeerIpv6NextHop
```

ipv6 bgp neighbor admin-state

Enables or disables the BGP peer status. These peers are identified by their IPv6 addresses.

```
ipv6 bgp neighbor ipv6_address [admin-state {enable | disable}]
```

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address of the new BGP peer.
enable	Enables the BGP peer.
disable	Disables the BGP peer.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You should first create a BGP peer and assign it an IPv6 address using the [ipv6 bgp neighbor](#) command before enabling the peer.
- You should configure all the BGP peer related commands before enabling a BGP peer. Once you have enabled the peer, it will begin sending BGP connection and route advertisement messages.

Examples

```
-> ipv6 bgp neighbor 2001::1 admin-state enable  
-> ipv6 bgp neighbor 2001::1 admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 bgp neighbors](#) Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table  
  alaBgpPeer6Addr  
  alaBgpPeer6RowStatus
```

ipv6 bgp neighbor remote-as

Assigns an AS number to the BGP peer.

```
ipv6 bgp neighbor ipv6_address [remote-as num]
```

Syntax Definitions

ipv6_address The 128-bit IPv6 address of the BGP peer.

num Autonomous system number in the range 1–65535.

Defaults

parameter	default
<i>num</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A BGP peer created with the **ipv6 bgp neighbor** command cannot be enabled until it is assigned an autonomous system number. If the AS number assigned to the peer matches the AS number of the local BGP speaker (assigned using the **ip bgp autonomous-system** command), the peer is considered internal to the local autonomous system. Otherwise, the peer is considered external to the local BGP speaker's AS.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::1 remote-as 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp autonomous-system Sets the AS for the local BGP speaker.

MIB Objects

```
alaBgpPeer6Table  
  alaBgpPeer6Addr  
  alaBgpPeer6AS
```

ipv6 bgp neighbor timers

Configures the KEEPALIVE message interval and hold time interval (in seconds) with regards to the specified BGP peer.

ipv6 bgp neighbor *ipv6_address* [**timers** *num num*]

Syntax Definitions

<i>ipv6_address</i>	A 128-bit IPv6 address for the BGP peer.
<i>num</i>	The KEEPALIVE message interval in seconds.
<i>num</i>	The hold time interval in seconds.

Defaults

parameter	default
<i>num</i> (keepalive)	30 seconds
<i>num</i> (holdtime)	90 seconds

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- KEEPALIVE messages do not contain route updates or indicate a change in the status of the BGP peer; they indicate to the receiving BGP peer that the connection is still live and the peer is reachable.
- By default, the KEEPALIVE interval of 30 seconds is one-third the default hold time interval of 90 seconds. The KEEPALIVE interval can never be more than one-third the value of the hold time interval. When the hold time interval is reached without receiving KEEPALIVE or other updates messages, the peer is considered dead.
- Setting the KEEPALIVE value to zero means no KEEPALIVE messages will be sent.
- Once a connection is established with a peer and a time period of the length specified in this command transpires with no messages from the remote peer, then the connection with that remote peer will be considered dead.
- The hold timer is used during the connection setup process and for on-going connection maintenance with BGP peers. If the peer does not receive a KEEPALIVE, UPDATE, or NOTIFICATION message within this time period, then the BGP connection will be closed.
- Both the KEEPALIVE and hold time interval should be set at the same time.
- Using this command without the variables resets the variables to their default value.

Examples

```
-> ipv6 bgp neighbor 2001::1 timers 80 240
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 bgp neighbor conn-retry-interval The interval, in seconds, between BGP retries to set up a connection with another peer through the transport protocol.

MIB Objects

alaBgpPeer6Table
 alaBgpPeer6Addr
 alaBgpPeer6HoldTime
 alaBgpPeer6KeepAlive

ipv6 bgp neighbor maximum-prefix

Configures the maximum number of prefixes, or paths, the local router can receive from a BGP peer in UPDATE messages.

```
ipv6 bgp neighbor ipv6_address [maximum-prefix num [warning-only]]
```

```
no ipv6 bgp neighbor ipv6_address [maximum-prefix num [warning-only]]
```

Syntax Definitions

ipv6_address A 128-bit IPv6 address for the BGP peer.

num The number of prefixes. The valid range is 0–4294967295.

Defaults

parameter	default
<i>num</i>	5000

By default, **warning-only** is enabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When the number of prefixes sent by the BGP peer reaches the maximum limit, the peer is restarted.
- You can use BGP logging to receive a warning when the number of prefixes received from the peer reaches 80 percent of the value you configure in this command.
- If the **warning-only** prefix is used, the operator will be warned when the peer exceeds 80 percent of the configured number of maximum prefixes.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::2 maximum-prefix 1000 warning-only  
-> no ipv6 bgp neighbor 2001::2 maximum-prefix 1000
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors Displays the configured IPv6 BGP peers.

MIB Objects

alaBgpPeer6Table

 alaBgpPeer6Addr

 alaBgpPeer6MaxPrefix

 alaBgpPeer6MaxPrefixWarnOnly

ipv6 bgp neighbor next-hop-self

Configures router to advertise its peering address as the next hop address for the specified neighbor.

```
ipv6 bgp neighbor ipv6_address [next-hop-self]
```

```
no ipv6 bgp neighbor ipv6_address [next-hop-self]
```

Syntax Definitions

ipv6_address A 128-bit IPv6 address for the BGP peer.

Defaults

By default, the **next-hop-self** parameter of BGP updates is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable the **next-hop-self** parameter.
- In meshed networks, the BGP peer may not have direct connections to other peers. When such a peer receives route updates from these distant peers (through other peers), it may treat the remote peer as if it were the next hop in the routing path. Packet forwarding will not work in such a case because no direct connection exists. This command allows the peer to deem itself the next hop on the routing path so that the two non-connected peers can route packets. This peer would have a direct connection to both peers that want to exchange packets.
- The BGP peer is restarted after issuing this command.

Examples

```
-> ipv6 bgp neighbor 2001::2 next-hop-self  
-> no ipv6 bgp neighbor 2001::2 next-hop-self
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 bgp neighbors](#) Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table  
  alaBgpPeer6Addr  
  alaBgpPeer6NextHopSelf
```

ipv6 bgp neighbor conn-retry-interval

The interval, in seconds, between BGP retries to set up a connection with another peer through the transport protocol. In the connect state, BGP tries to set up a connection with a remote peer. If the connection fails, then the connection retry interval starts. Once this interval elapses, BGP retries setting up the connection.

ipv6 bgp neighbor *ipv6_address* [**conn-retry-interval** *num*]

Syntax Definitions

<i>ipv6_address</i>	A 128-bit IPv6 address for the BGP neighbor.
<i>num</i>	The time interval (in seconds) between retries. The valid range is 0–65535.

Defaults

parameter	default
<i>num</i>	120

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The connection retry time interval starts when a connection to a peer is lost.
- Using this command without the *num* variable resets the variable to its default value.

Examples

```
-> ipv6 bgp neighbor 2001::2 conn-retry-interval 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 bgp neighbors](#) Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table  
  alaBgpPeer6Addr  
  alaBgpPeer6ConnRetryInterval
```

ipv6 bgp neighbor default-originate

Enables or disables the BGP local speaker to advertise a default route to the peer.

```
ipv6 bgp neighbor ipv6_address [default-originate]
```

```
no ipv6 bgp neighbor ipv6_address [default-originate]
```

Syntax Definitions

ipv6_address The 128-bit IPv6 address for the neighbor.

Defaults

This **default-originate** parameter is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable the BGP peer default origination.
- When this command is enabled, the local BGP speaker advertises the default route to the peer. Such a default route overrides any learned default (propagation) and outbound policy. The default route `::/0` does not need to exist on the local router.
- If the peer is capable of exchanging IP as well as IPv6 prefixes, the default route for both IP and IPv6 is advertised.

Examples

```
-> ipv6 bgp neighbor 2001::1 default-originate  
-> no ipv6 bgp neighbor 2001::1 default-originate
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 bgp neighbors](#) Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table  
  alaBgpPeer6Addr  
  alaBgpPeer6DefaultOriginate
```

ipv6 bgp neighbor update-source

Configures the local IPv6 interface from which a BGP peer will be connected. This local IPv6 interface can be configured for internal and external BGP peers.

ipv6 bgp neighbor *ipv6_address* [**update-source** *interface_name*]

no ipv6 bgp neighbor *ipv6_address* [**update-source** *interface_name*]

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address for the BGP peer.
<i>interface_name</i>	The name of the local IPv6 interface that provides the TCP connection for this BGP peer.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The BGP peer is restarted after issuing this command.
- If a BGP peer is configured with its link-local address, use the **update-source** parameter to specify the name of the IPv6 interface from which this peer is reachable. This is required to establish a BGP peering session.

Examples

```
-> ipv6 bgp neighbor 2004::1 update-source bgp_ipv6  
-> no ipv6 bgp neighbor 2004::1 update-source bgp_ipv6
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors	Displays the configured IPv6 BGP peers.
ipv6 interface	Configures an IPv6 interface on a VLAN or IPv6 tunnel.

MIB Objects

```
alaBgpPeer6Table  
  alaBgpPeer6Addr  
  alaBgpPeer6LocalIntfName
```

ipv6 bgp neighbor ipv4-nexthop

Configures the IPv4 next hop addresses for IPv4 prefixes advertised between BGP peers. These BGP peers are identified by their IPv6 addresses.

```
ipv6 bgp neighbor ipv6_address [ipv4-nexthop ip_address]
```

Syntax Definitions

<i>ipv6_address</i>	The 128-bit IPv6 address for the BGP peer.
<i>ip_address</i>	The 32-bit IP address of the next hop.

Defaults

By default, the IPv4 next hop value is set to all zeros.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

To reset the IPv4 next hop value, enter an all-zero address.

Examples

```
-> ipv6 bgp neighbor 2004::1 ipv4-nexthop 172.22.2.115  
-> ipv6 bgp neighbor 2004::1 ipv4-nexthop 0.0.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 bgp neighbors](#) .Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table  
  alaBgpPeer6Addr  
  alaBgpPeer6Ipv4NextHop
```

show ipv6 bgp neighbors

Displays the configured IPv6 BGP peers.

show ipv6 bgp neighbors [*ipv6_address*]

Syntax Definitions

ipv6_address The 128-bit IPv6 address of the BGP neighbor.

Defaults

By default, all the configured IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *ipv6_address* parameter to display the details of a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors
```

```
Legends: Nbr = Neighbor
```

```
      As = Autonomous System
```

Nbr	address	As	Admin state	Oper state	BGP Id	Up/Down
2001:100:3:4::1		30	enabled	established	11.4.0.1	01h:42m:08s
fe80::200:57ff:fe28:7e89		10	enabled	established	11.5.0.1	01h:40m:58s

```
-> show ipv6 bgp neighbors 2001:100:3:4::1
```

```
Neighbor address                      = 2001:100:3:4::1,
Neighbor autonomous system            = 30,
Neighbor Admin state                  = enabled,
Neighbor Oper state                    = established,
Neighbor passive status                = disabled,
Neighbor name                          = peer(2001:100:3:4::1),
Neighbor local address                 = 2001:100:3:4::10,
Neighbor EBGP multiHop                 = disabled,
Neighbor next hop self                 = disabled,
Neighbor Route Refresh                 = enabled,
Neighbor Ipv4 unicast                 = enabled,
Neighbor Ipv4 multicast                = disabled,
Neighbor type                          = internal,
Neighbor auto-restart                  = enabled,
Neighbor route-reflector-client        = disabled,
Neighbor confederation status          = disabled,
Neighbor remove private AS             = disabled,
Neighbor default originate             = disabled,
Neighbor maximum prefixes              = 5000,
Neighbor max prefixes warning          = enabled,
# of prefixes received                 = 10,
```

```

Neighbor MD5 key           = <none>,
Neighbor local port        = 49154,
Neighbor TCP window size   = 32768,
Graceful Restart State     = None,
Advertised Restart Interval = 0s,
Forwarding State during restart = NotPreserved,
Activate IPv6 unicast      = enabled,
Configured IPv4 NextHop Address = 0.0.0.0,
Configured IPv6 NextHop Address = ::,
Neighbor Ipv6 unicast      = advertised

```

output definitions

Nbr address or Neighbor address	The IPv6 address for this BGP peer. Assign this address through the ipv6 bgp neighbor command.
As or Neighbor autonomous system	The autonomous system to which this peer belongs. A peer's AS number is assigned through the ipv6 bgp neighbor remote-as command.
Admin state or Neighbor Admin state	Indicates whether this peer has been enabled or disabled through the ipv6 bgp neighbor admin-state command.
Oper state or Neighbor Oper state	The current BGP state for this peer. Possible states are idle , connect , active , opensent , openconfirm , and established .
BGP Id	The unique BGP identifier of the peer.
Up/Down	The time since this peer has transitioned to its current UP or DOWN state. If the peer is currently Established, then this is the time that the peer has been UP. If the peer is currently Idle, then this is the time the peer has been DOWN.
Neighbor passive status	Indicates whether the local BGP speaker is "passive" (i.e., waiting for this peer to initiate a session).
Neighbor name	The name assigned to this peer.
Neighbor local address	The interface assigned to this peer. This value is configured through the ipv6 bgp neighbor update-source command.
Neighbor EBGp multiHop	Indicates whether BGP multi-hop support is enabled or disabled. This supports allows external BGP peers to communicate with each other even when they are not directly connected.
Neighbor next hop self	Indicates whether this peer is using next hop processing. This value is configured through the ipv6 bgp neighbor next-hop-self command.
Neighbor Route Refresh	Indicates whether this peer supports Route Refresh capability as defined in RFC 2918. This capability is an alternative to soft-reconfiguration that can save CPU and memory resources. It allows peers to dynamically request the re-advertisement of BGP routing tables. Since this router supports route refresh all BGP peers are automatically enabled for this capability.
Neighbor Ipv4 unicast	Indicates whether this peer is multiprotocol IPv4 unicast capable.
Neighbor Ipv4 multicast	Indicates whether this peer is multiprotocol IPv4 multicast capable.
Neighbor type	Indicates whether this peer is internal or external to the AS.
Neighbor auto-restart	Indicates whether peer auto-restart is enabled or disabled.

output definitions (continued)

Neighbor route-reflector-client	Indicates whether this peer is a client to the local route reflector, if configured.
Neighbor confederation status	Indicates whether this peer is a member of a BGP confederation.
Neighbor remove private AS	Indicates whether the stripping of private AS numbers (64512 to 65535) from AS paths is enabled or disabled.
Neighbor default originate	Indicates whether peer default origination is enabled or disabled. When enabled, the local BGP speaker advertises the default route to the peer. This value is configured through the ipv6 bgp neighbor default-originate command.
Neighbor maximum prefixes	The maximum number of prefixes the local router can receive in UPDATE from this peer. This value is configured through the ipv6 bgp neighbor maximum-prefix command.
Neighbor max prefixes warning	Indicates whether a warning will be issued when this peer exceeds 80 percent of the maximum prefix value. This value is configured through the ipv6 bgp neighbor update-source command.
# of prefixes received	Displays the total number of prefixes received by this neighbor.
Neighbor MD5 key	When present, shows an encrypted version of the MD5 password. When not present, and MD5 password has not been configured.
Neighbor local port	The TCP port used for the session with this peer.
Neighbor TCP window size	The size of the TCP window for this BGP session. This value will always be 32768 as that is the maximum size of a BGP message.
Graceful Restart State	Indicates the graceful restart state. This feature does not support IPv6 prefixes.
Advertised Restart Interval	Indicates the restart interval in seconds.
Forwarding State during restart	Indicates whether the peer has preserved the forwarding state during the graceful restart.
Activate IPv6 unicast	Indicates whether or not IPv6 unicast advertisements are enabled. Options include enabled or disabled .
Configured IPv4 NextHop Address	Specifies the IPv4 nexthop address. This is specified using the ipv6 bgp neighbor ipv4-nexthop command.
Configured IPv6 NextHop Address	Specifies the IPv6 nexthop address. This is specified using the ipv6 bgp neighbor ipv6-nexthop command.
Neighbor Ipv6 unicast	Indicates whether or not IPv6 unicast capability is advertised between the peers. Options include enabled or disabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

- ipv6 bgp neighbor** Creates or deletes a BGP peer relationship using IPv6 addresses
- ipv6 bgp neighbor admin-state** Enables or disables the BGP peer status.

MIB Objects

```
alaBgpPeer6Table
  alaBgpPeer6Addr
  alaBgpPeer6AS
  alaBgpPeer6Passive
  alaBgpPeer6Name
  alaBgpPeer6MultiHop
  alaBgpPeer6MaxPrefix
  alaBgpPeer6MaxPrefixWarnOnly
  alaBgpPeer6NextHopSelf
  alaBgpPeer6SoftReconfig
  alaBgpPeer6InSoftReset
  alaBgpPeer6Ipv4Unicast
  alaBgpPeer6Ipv4Multicast
  alaBgpPeer6RcvdRtRefreshMsgs
  alaBgpPeer6SentRtRefreshMsgs
  alaBgpPeer6RouteMapOut
  alaBgpPeer6RouteMapIn
  alaBgpPeer6LocalAddr
  alaBgpPeer6LastDownReason
  alaBgpPeer6LastDownTime
  alaBgpPeer6LastReadTime
  alaBgpPeer6RcvdNotifyMsgs
  alaBgpPeer6SentNotifyMsgs
  alaBgpPeer6LastSentNotifyReason
  alaBgpPeer6LastRecvNotifyReason
  alaBgpPeer6RcvdPrefixes
  alaBgpPeer6DownTransitions
  alaBgpPeer6Type
  alaBgpPeer6AutoRestart
  alaBgpPeer6ClientStatus
  alaBgpPeer6ConfedStatus
  alaBgpPeer6RemovePrivateAs
  alaBgpPeer6ClearCounter
  alaBgpPeer6TTL
  alaBgpPeer6AspathListOut
  alaBgpPeer6AspathListIn
  alaBgpPeer6PrefixListOut
  alaBgpPeer6PrefixListIn
  alaBgpPeer6CommunityListOut
  alaBgpPeer6CommunityListIn
  alaBgpPeer6Restart
  alaBgpPeer6DefaultOriginate
  alaBgpPeer6ReconfigureInBound
  alaBgpPeer6ReconfigureOutBound
  alaBgpPeer6MD5Key
  alaBgpPeer6MD5KeyEncrypt
  alaBgpPeer6RowStatus
  alaBgpPeer6UpTransitions
  alaBgpPeer6LastWriteTime
  alaBgpPeer6AdminStatus
```



```
alaBgpPeer6State  
alaBgpPeer6LocalPort  
alaBgpPeer6TcpWindowSize  
alaBgpPeer6ActivateIpv6
```

show ipv6 bgp neighbors statistics

Displays the neighbor statistics of the configured IPv6 BGP peers.

show ipv6 bgp neighbors statistics [*ipv6_address*]

Syntax Definitions

ipv6_address The 128-bit IPv6 address.

Defaults

By default, the neighbor statistics for all the IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *ipv6_address* parameter to display the neighbor statistics of a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors statistics
```

```
Legends: Nbr    = Neighbor
          As     = Autonomous System
          RMSGS  = # of received messages
          SMSGS  = # of sent messages
          RUPDS  = # of Update messages received
          SUPDS  = # of Update messages sent
          RNOFY  = # of Notify messages received
          SNOFY  = # of Notify messages sent
          RPFXS  = # of prefixes received
          UPTNS  = # of UP transitions
          DNTNS  = # of DOWN transitions
```

```
Nbr address           As     RMSGS SMSGS RUPDS SUPDS RNOFY SNOFY RPFXS UPTNS DNTNS
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
2001:100:3:4::1      30     225  260   2     3     0     0     10    1     1
```

output definitions

Nbr address	The IPv6 address for this peer. This value is configured using the ipv6 bgp neighbor command.
As	The autonomous system to which this peer belongs. This value is configured using the ipv6 bgp neighbor remote-as command.
RMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.
SMSGS	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent by this peer.

output definitions (continued)

RUPDS	The number of route UPDATE messages received by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
SUPDS	The number of route UPDATE messages sent by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
RNOFY	The number of NOTIFY messages received by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
SNOFY	The number of NOTIFY messages sent by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
RPFXS	Number of unique route prefixes received by this peer.
UPTNS	Number of times this peer has come up, operationally.
DNTNS	Number of times this peer has gone down, operationally.

```
-> show ipv6 bgp neighbors statistics 2001:100:3:4::1
Neighbor address           = 2001:100:3:4::1,
# of UP transitions        = 1,
Time of last UP transition = 01h:50m:36s,
# of DOWN transitions      = 1,
Time of last DOWN transition = 00h:00m:00s,
Last DOWN reason          = none,
# of msgs rcvd            = 226,
# of Update msgs rcvd     = 2,
# of prefixes rcvd       = 10,
# of Route Refresh msgs rcvd = 0,
# of Notification msgs rcvd = 0,
Last rcvd Notification reason = none [none]
Time last msg was rcvd     = 00h:00m:04s,
# of msgs sent            = 260,
# of Update msgs sent     = 3,
# of Route Refresh msgs sent = 0
# of Notification msgs sent = 0,
Last sent Notification reason = none [none]
Time last msg was sent     = 00h:00m:18s,
```

output definitions

Neighbor address	The IPv6 address for this peer. This value is configured using the ipv6 bgp neighbor command.
# of UP transitions	Number of times this peer has come up, operationally.
Time of last UP transition	The duration that this peer has been up.
# of DOWN transitions	Number of times this peer has gone down, operationally.
Time of last DOWN transition	The duration since this peer last went down.

output definitions (continued)

Last DOWN reason	Provides a message as the last reason why a peer went down. The possible reasons for going down are: user_request - user initiated conn_timeout - connection timer expired hold_timeout - hold timer expired bad_msg - received a bad message from neighbor fsm_blink - BGP FSM error peer_closed - neighbor closed connection peer_notify - neighbor sent fatal notification tcp_error - Fatal TCP error none - None
# of msgs rcvd	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.
# of Update msgs rcvd	The number of route UPDATE messages received from this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of prefixes rcvd	Number of unique route prefixes received by this peer.
# of Route Refresh msgs rcvd	Number of route refresh requests this peer has received. Route refresh requests all routes learned by a peer.
# of Notification msgs rcvd	Number of NOTIFY messages received from this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last rcvd Notification reason	<p>NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message received from this peer. The notification reasons are listed in two parts separated by a dash (-). The following are possible notification reasons:</p> <ul style="list-style-type: none"> message header error - synchronization loss message header error - bad length message header error - bad type open message error - unsupported version open message error - bad peer autonomous system open message error - bad peer bgp id open message error - unsupported option open message error - authentication failure open message error - unacceptable hold time open message error - unsupported capability update message error - malformed attribute update message error - unknown attribute update message error - missing wellknown attribute update message error - attribute flags error update message error - attribute length error update message error - invalid origin update message error - as loop update message error - invalid nexthop update message error - optional attribute error update message error - invalid network update message error - malformed aspath cease - maximum number of prefixes reached cease - administrative shutdown cease - peer de-configured cease- administrative reset cease- connection rejected cease - other configuration change cease - connection collision resolution cease - out of resources hold time out - none fsm error - none none - none
Time last msg was rcvd	The duration since a message was received from this peer.
# of msgsd sent	Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent to this peer.
# of Update msgsd sent	Number of route UPDATE messages sent to this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.
# of Route Refresh msgsd sent	Number of route refresh requests this peer has sent. Route refresh requests request all routes learned be a peer.
# of Notification msgsd sent	Number of NOTIFY messages sent to this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.

output definitions (continued)

Last sent Notification reason	NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message sent by this peer. The notification reasons are listed in two parts separated by a dash (-). See the list of possible notification reasons under the description for the Peer last received notification reason field above.
Time last msg was sent	The duration since a message was sent to this peer.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors Displays the configured IPv6 BGP peers.

MIB Objects

```
alaBgpPeer6Table
  alaBgpPeer6Addr
  alaBgpPeer6RcvdMsgs
  alaBgpPeer6SentMsgs
  alaBgpPeer6RcvdUpdMsgs
  alaBgpPeer6SentUpdMsgs
  alaBgpPeer6LastTransitionTime
  alaBgpPeer6LastUpTime
  alaBgpPeer6BgpId
  alaBgpPeer6LocalIntfName
  alaBgpPeer6RestartTime
  alaBgpPeer6RestartState
  alaBgpPeer6RestartFwdState
  alaBgpPeer6Ipv6Unicast
  alaBgpPeer6HoldTime
  alaBgpPeer6KeepAlive
  alaBgpPeer6ConnRetryInterval
  alaBgpPeer6HoldTimeConfigured
  alaBgpPeer6KeepAliveConfigured
  alaBgpPeer6Ipv4NextHop
  alaBgpPeer6Ipv6NextHop
```

show ipv6 bgp neighbors policy

Displays the incoming and outgoing prefix6 list policy identifiers configured for BGP IPv6 peer.

```
show ipv6 bgp neighbors policy ipv6_address
```

Syntax Definitions

ipv6_address The 128-bit IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays all of the configured policies for the router, or the policies configured for a specific BGP IPv6 peer.

Examples

```
OS6850::> show ipv6 bgp neighbors policy
Neighbor address = 2001::1,
  Neighbor autonomous system      = 1,
  Neighbor output policy map name = <none>,
  Neighbor input policy map name  = <none>,
  Neighbor output aspath-list name = <none>,
  Neighbor input aspath-list name = <none>,
  Neighbor output prefix-list name = <none>,
  Neighbor input prefix-list name = <none>,
  Neighbor output community-list name = <none>,
  Neighbor input community-list name = <none>,
  Neighbor soft reconfiguration   = enabled
  Neighbor output prefix6-list name = <none>,
  Neighbor input prefix6-list name = <none>
```

output definitions

Neighbor autonomous system	The AS to which the peer is assigned. This can be assigned by using the ip bgp neighbor remote-as command.
Neighbor output policy map name	The outbound route map policy for the peer. This can be assigned by using the ip bgp neighbor route-map command.
Neighbor input policy map name	The inbound route map policy for the peer. This can be assigned by using the ip bgp neighbor route-map command.
Neighbor output aspath-list name	The outbound AS path list policy for the peer. This can be assigned by using the ip bgp neighbor out-aspathlist command.
Neighbor input aspath-list name	The inbound AS path list policy for the peer. This can be assigned by using the ip bgp neighbor in-aspathlist command.

output definitions (continued)

Neighbor output prefix-list name	The outbound prefix list policy for the peer. This can be assigned by using the ip bgp neighbor out-prefixlist command.
Neighbor input prefix-list name	The inbound prefix list policy for the peer. This can be assigned by using the ip bgp neighbor in-prefixlist command.
Neighbor output community-list name	The outbound community list policy for the peer. This can be assigned by using the ip bgp neighbor out-communitylist command.
Neighbor input community-list name	The inbound community list policy for the peer. This can be assigned by using the ip bgp neighbor in-communitylist command.
Neighbor soft reconfiguration	Lists whether soft reconfigurations are enabled or disabled for this peer. This is configured using the ip bgp neighbor soft-reconfiguration command.
Neighbor output prefix6-list name	The outbound prefix6-list policy for the peer.
Neighbor input prefix6-list name	The inbound prefix6-list policy for the peer.

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 bgp neighbors Displays configured IPv6 BGP peers

MIB Objects

alaBgpPeer6Table
 alaBgpPeer6Prefix6ListIn
 alaBgpPeer6Prefix6ListOut

show ipv6 bgp neighbors timers

Displays the timers for configured IPv6 BGP peers.

show ipv6 bgp neighbors timers [*ipv6_address*]

Syntax Definitions

ipv6_address The 128-bit IPv6 address.

Defaults

By default, the timer values for all the IPv6 BGP peers will be displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *ipv6_address* parameter to display the timer value for a specified IPv6 BGP peer.

Examples

```
-> show ipv6 bgp neighbors timers
Legends: Nbr      = Neighbor
          As       = Autonomous System
          RtAdv    = Route Advertisement
          Kalive   = Keep Alive (actual)
          Ka(C)    = Configured Keep Alive

Nbr address                As      Hold   Hold(C) RtAdv  Retry  Kalive  Ka(C)
-----+-----+-----+-----+-----+-----+-----+-----
2001:100:3:4::1           30     90     90      30    120    30     30
```

output definitions

Nbr address	The IPv6 address for this BGP peer. Assign this address using the ipv6 bgp neighbor command.
As	The autonomous system to which this peer belongs. A peer's AS number is assigned using the ipv6 bgp neighbor remote-as command.
Hold	The actual negotiated hold time value.
Hold (C)	The hold time value. This value is configured using the ipv6 bgp neighbor timers command.
RtAdv	The route advertisement interval, in seconds, for updates between external BGP peers.
Retry	The interval, in seconds, between retries by this peer to set up a connection through TCP with another peer. This value is configured using the ipv6 bgp neighbor timers command.

output definitions (continued)

Kalive	The actual negotiated value, in seconds, between KEEPALIVE messages. KEEPALIVE messages do not contain route or status updates; they serve only to tell other peers that the connection is still live and this peer is reachable.
Ka (C)	The KEEPALIVE interval as configured using the ipv6 bgp neighbor timers command.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip bgp statistics](#) Displays BGP global statistics.

MIB Objects

alaBgpPeer6Table
 alaBgpPeer6Addr
 alaBgpPeer6ConnRetryInterval
 alaBgpPeer6MinRouteAdvertisementInterval
 alaBgpPeer6HoldTime

23 Server Load Balancing Commands

Server Load Balancing (SLB) allows clients to send requests to servers logically grouped together in clusters. Each cluster logically aggregates a set of servers running identical applications with access to the same content (for example, web servers). Clients access clusters through the use of a Virtual IP (VIP) address.

MIB information for the SLB commands is as follows:

Filename AlcatellIND1Slb.mib
Module: ALCATEL-IND1-SLB-MIB

A summary of available commands is listed here:

Global SLB Commands	<code>ip slb admin-state</code> <code>ip slb reset statistics</code> <code>show ip slb</code>
SLB Cluster Commands	<code>ip slb cluster</code> <code>ip slb cluster admin-state</code> <code>ip slb cluster ping period</code> <code>ip slb cluster ping timeout</code> <code>ip slb cluster ping retries</code> <code>ip slb cluster probe</code> <code>show ip slb clusters</code> <code>show ip slb cluster</code>
SLB Server Commands	<code>ip slb server ip cluster</code> <code>ip slb server ip cluster probe</code> <code>show ip slb cluster server</code> <code>show ip slb servers</code>
SLB Probe Commands	<code>ip slb probe</code> <code>ip slb probe timeout</code> <code>ip slb probe period</code> <code>ip slb probe port</code> <code>ip slb probe retries</code> <code>ip slb probe username</code> <code>ip slb probe password</code> <code>ip slb probe url</code> <code>ip slb probe status</code> <code>ip slb probe send</code> <code>ip slb probe expect</code> <code>show ip slb probes</code>

ip slb admin-state

Enables or disables the administrative status for Server Load Balancing (SLB) on a switch.

ip slb admin-state {enable | disable}

Syntax Definitions

enable	Enables the administrative status for Server Load Balancing on a switch.
disable	Disables the administrative status for Server Load Balancing on the switch.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Disabling the administrative status for the SLB feature does not delete the SLB configuration from the switch. The next time the feature is enabled, the existing configuration becomes active.

Examples

```
-> ip slb admin-state enable
-> ip slb admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb	Displays the status of Server Load Balancing on a switch.
ip slb cluster	Configures a Server Load Balancing cluster on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbFeatureGroup
  slbAdminStatus
```

ip slb reset statistics

Resets SLB statistics for all clusters configured on the switch.

ip slb reset statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Note that the **qos apply** command resets both QoS statistics *and* SLB cluster statistics. The **ip slb reset statistics** command only resets SLB statistics.

Examples

```
-> ip slb reset statistics
```

Release History

Release 7.1.1; command introduced.

Related Commands

- | | |
|--------------------------------------|--|
| show ip slb clusters | Displays the status and configuration of all Server Load Balancing clusters on a switch. |
| show ip slb cluster | Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch. |

MIB Objects

```
slbFeatureGroup  
  slbResetStatistics
```

ip slb cluster

Configures a Server Load Balancing (SLB) cluster on a switch.

ip slb cluster *name* {**vip** *ip_address* | **condition** *string*} [**I3** | **I2**]

no ip slb cluster *name*

Syntax Definitions

<i>name</i>	The name of the Server Load Balancing (SLB) cluster. The name can consist a maximum of 23 characters. Names with spaces must be enclosed within quotation marks (for example, “mail server”).
<i>ip_address</i>	The Virtual IP (VIP) address for the Server Load Balancing cluster. This IP address must be in dotted decimal format.
<i>string</i>	The name of an existing QoS policy condition that identifies the Server Load Balancing cluster.
I3	Specifies Layer 3 Server Load Balancing mode. The source and destination MAC and TTL of each packet is modified before the packet is bridged or routed to the server.
I2	Specifies Layer 2 Server Load Balancing mode. Packets are not modified before they are bridged to the server. This parameter is only available when using the condition parameter.

Defaults

parameter	default
I3 I2	I3

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a Server Load Balancing cluster.
- Once a cluster is created, the Virtual IP or condition cannot be modified. To modify these values, delete the cluster and re-create the cluster with the different VIP and conditions.
- The VIP address of the SLB cluster *must* be an address that is in the same subnet as the servers. In addition, do not specify a VIP address that is already in use by an MCLAG VIP interface. The SLB VIP and MCLAG VIP both provide a common IP address but for different entities and should not share the same IP address.
- Specifying the **I3** parameter when configuring a VIP cluster is not required. VIP clusters only use the Layer-3 mode to route traffic to the servers. Layer-2 mode is not supported with this type of cluster.

- The QoS policy condition must exist before it is assigned to an SLB cluster. Use the **policy condition** command to create the QoS policy condition. See the “QoS Policy Commands” chapter for more information.
- SLB clusters are not active if the Server Load Balancing feature is disabled for the switch. Use the **ip slb admin-state** command to enable this feature.

Note

It is possible to configure clusters and add or remove servers from a cluster even when SLB is disabled for the switch.

Examples

```
-> ip slb cluster corporate_servers vip 1.2.3.4
-> ip slb cluster "mail servers" vip 1.2.3.6
-> ip slb cluster cluster_1 condition intranet_cond 12
-> ip slb cluster cluster_2 condition slb_cond 13
-> no ip slb cluster hr_servers
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb admin-state	Enables or disables Server Load Balancing on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbClusterTable
  slbClusterName
  slbClusterVIP
  slbClusterRowStatus
  slbClusterPackets
  slbClusterCondition
  slbClusterType
```

ip slb cluster admin-state

Administratively enables or disables a Server Load Balancing (SLB) cluster on a switch.

```
ip slb cluster cluster_name admin-state {enable | disable}
```

Syntax Definitions

<i>cluster_name</i>	The name of an existing Server Load Balancing cluster.
enable	Administratively enables a Server Load Balancing cluster on a switch.
disable	Administratively disables a Server Load Balancing cluster on a switch.

Defaults

By default, a cluster is administratively enabled when the cluster is created.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The SLB cluster name specified with this command must already exist in the switch configuration.

Examples

```
-> ip slb cluster hr_servers admin-state enable
-> ip slb cluster "mail servers" admin-state disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster	Configures Server Load Balancing clusters.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

```
slbClusterTable
    slbClusterAdminStatus
```

ip slb cluster ping period

Modifies the number of seconds to check the health of the servers in a Server Load Balancing cluster.

ip slb cluster *cluster_name* **ping period** *seconds*

Syntax Definitions

<i>cluster_name</i>	The name of the Server Load Balancing (SLB) cluster.
<i>seconds</i>	The number of seconds for the ping period. Specifying 0 (zero) disables the ping.

Defaults

parameter	default
<i>seconds</i>	60

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you do not set the ping period to zero, then the ping period *must* be greater than or equal to the ping timeout value divided by 1000. Use the [ip slb cluster ping timeout](#) command to modify the ping timeout value.

Examples

```
-> ip slb cluster hr_servers ping period 120
-> ip slb cluster "mail servers" ping period 0
```

Release History

Release 7.1.1; command introduced.

Related Commands**show ip slb clusters**

Displays the status and configuration of all Server Load Balancing clusters on a switch.

show ip slb cluster

Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.

ip slb cluster ping timeout

Modifies the ping timeout value.

ip slb cluster ping retries

Modifies the number of ping retries.

MIB Objects

slbClusterTable

 slbClusterPingPeriod

ip slb cluster ping timeout

Configures the ping timeout value for a Server Load Balancing (SLB) cluster before it retries.

ip slb cluster *cluster_name* **ping timeout** *milliseconds*

Syntax Definitions

<i>cluster_name</i>	The name of the Server Load Balancing (SLB) cluster.
<i>milliseconds</i>	The number of milliseconds for the ping timeout. The valid range for the ping timeout value is 0 to 1000 times the ping period. For example, if the ping period is 10 seconds, then maximum value for the ping timeout is 10000.

Defaults

parameter	default
<i>milliseconds</i>	3000

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the [ip slb cluster ping period](#) command to modify the ping period value.

Examples

```
-> ip slb cluster "mail servers" ping timeout 1000
-> ip slb cluster hr_servers ping timeout 6000
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb cluster ping period	Modifies the ping period value.
ip slb cluster ping retries	Modifies the number of ping retries.

MIB Objects

```
slbClusterTable  
    slbClusterPingTimeout
```

ip slb cluster ping retries

Configures the number of ping attempts for a Server Load Balancing (SLB) cluster.

ip slb cluster *cluster_name* **ping retries** *count*

Syntax Definitions

cluster_name The name of the Server Load Balancing (SLB) cluster.

count The number of ping retries.

Defaults

parameter	default
<i>count</i>	3

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb cluster "mail servers" ping retries 5
-> ip slb cluster hr_servers ping retries 10
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show ip slb clusters](#) Displays the status and configuration of all Server Load Balancing clusters on a switch.

[show ip slb cluster](#) Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.

[ip slb cluster ping period](#) Modifies the ping period value.

[ip slb cluster ping timeout](#) Modifies the ping timeout value.

MIB Objects

slbClusterTable
 slbClusterPingRetries

ip slb cluster probe

Configures a probe for a Server Load Balancing (SLB) cluster.

```
ip slb cluster cluster_name probe probe_name
```

Syntax Definitions

<i>cluster_name</i>	The name of the Server Load Balancing (SLB) cluster.
<i>probe_name</i>	The name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

You must create the probe with the [ip slb probe](#) before you can use this command.

Examples

```
-> ip slb cluster mail_servers probe mail_server_probe
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
ip slb probe	Configures and deletes SLB probes.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb server ip cluster	Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

slbClusterTable
 slbClusterProbeName

ip slb server ip cluster

Adds a physical server to a Server Load Balancing (SLB) cluster, deletes a physical server from an SLB cluster, or modifies the administrative status of a physical server in an SLB cluster.

ip slb server ip *ip_address* **cluster** *cluster_name* [**admin-state** {**enable** | **disable**}] [**weight** *weight*]

no ip slb server ip *ip_address* **cluster** *cluster_name*

Syntax Definitions

<i>ip_address</i>	The IP address for the physical server.
<i>cluster_name</i>	The name of an existing Server Load Balancing cluster.
enable	Enables a server.
disable	Disables a server.
<i>weight</i>	Specifies the weight of the server.

Defaults

parameter	default
enable disable	enable
weight	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a physical server from a Server Load Balancing cluster.
- Use the **weight** parameter to assign the server preference value. Each server or server cluster can be assigned a weight to set their preference value for distribution of incoming network traffic. The weights assigned are relative. For example, if Servers A and B have respective weights of 10 and 20 within a cluster, Server A would get half the traffic of Server B.
- Assigning a weight of 0 (zero) to a server prevents the server from being assigned any new connections. This server is a backup server.
- A higher weight value indicates that the server can accept more network traffic.

Examples

```
-> ip slb server ip 10.255.11.127 cluster corporate_servers
-> ip slb server ip 10.255.11.109 cluster "mail servers" admin-state enable
weight 5
-> no ip slb server ip 10.255.11.105 cluster hr_servers
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb admin-state	Enables or disables Server Load Balancing on a switch.
ip slb cluster	Configures Server Load Balancing clusters.

MIB Objects

```
slbServerTable
  slbServerRowStatus
  slbServerAdminStatus
  slbServerAdminWeight
```

ip slb server ip cluster probe

Configures a probe for a Server Load Balancing (SLB) server.

```
ip slb server ip ip_address cluster cluster_name probe probe_name
```

Syntax Definitions

<i>ip_address</i>	The IP address for the physical server.
<i>cluster_name</i>	The name of the Server Load Balancing (SLB) cluster.
<i>probe_name</i>	The name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

You must create the probe with the [ip slb probe](#) before you can use this command.

Examples

```
-> ip slb server ip 10.255.11.127 cluster corporate_servers probe p_http
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
ip slb probe	Configures and deletes SLB probes.
ip slb admin-state	Enables or disables Server Load Balancing on a switch.
ip slb cluster	Configures Server Load Balancing clusters.

MIB Objects

slbServerTable
 slbServerProbeName

ip slb probe

Configures a Server Load Balancing (SLB) probe used to check the health of servers or clusters.

```
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
```

```
no ip slb probe probe_name
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to delete an SLB probe.

Examples

```
-> ip slb probe mail_server_probe smtp  
-> no ip slb probe mail_server_probe
```

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb probes

Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable  
  slbProbeName  
  slbProbeMethod
```

ip slb probe timeout

Configures the amount of time to wait for Server Load Balancing (SLB) probe answers.

```
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
timeout seconds
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
<i>seconds</i>	Specifies the timeout in seconds.

Defaults

parameter	default
<i>seconds</i>	3000

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb probe mail_server smtp timeout 12000
```

Release History

Release 7.1.1; command introduced.

Related Commands

[ip slb probe](#)

Configures and deletes SLB probes.

[show ip slb probes](#)

Displays the configuration of SLB probes.

MIB Objects

slbProbeTable

slbProbeName

slbProbeMethod

slbProbeTimeout

ip slb probe period

Configures the length of time between each SLB probe to check the health of the servers.

```
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
period seconds
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
<i>seconds</i>	Specifies the length of time for the SLB probe period.

Defaults

parameter	default
<i>seconds</i>	60

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http period 120
```

Release History

Release 7.1.1; command introduced.

Related Commands

[ip slb probe](#)

Configures and deletes SLB probes.

[show ip slb probes](#)

Displays the configuration of SLB probes.

MIB Objects

slbProbeTable

 slbProbeName

 slbProbeMethod

 slbProbePeriod

ip slb probe port

Configures the TCP/UDP port on which the Server Load Balancing (SLB) probe is sent.

```
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
port port_number
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
<i>port_number</i>	Specifies the TDP/UDP port number.

Defaults

parameter	default
<i>port_number</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb probe mis_server udp port 200
```


Release History

Release 7.1.1; command introduced.

Related Commands

[ip slb probe](#)

Configures and deletes SLB probes.

[show ip slb probes](#)

Displays the configuration of SLB probes.

MIB Objects

slbProbeTable

 slbProbeName

 slbProbeMethod

 slbProbePort

ip slb probe retries

Configures the number of Server Load Balancing (SLB) probe retries that are performed before deciding that a server is out of service.

ip slb probe *probe_name* {**ftp** | **http** | **https** | **imap** | **imaps** | **nntp** | **ping** | **pop** | **pops** | **smtp** | **tcp** | **udp**}
retries *retries*

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
ftp	Specifies an FTP probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
imap	Specifies an IMAP probe.
imaps	Specifies an IMAPS probe.
nntp	Specifies an NNTP probe.
ping	Specifies a ping probe.
pop	Specifies a POP probe.
pops	Specifies a POPS probe.
smtp	Specifies an SMTP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
<i>retries</i>	Specifies the number of retries.

Defaults

parameter	default
<i>retries</i>	3

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb probe mail_server smtp retries 5
```

Release History

Release 7.1.1; command introduced.

Related Commands

[ip slb probe](#)

Configures and deletes SLB probes.

[show ip slb probes](#)

Displays the configuration of SLB probes.

MIB Objects

slbProbeTable

 slbProbeName

 slbProbeMethod

 slbProbeRetries

ip slb probe username

Configures a user name that is sent to a server as credentials for an HTTP GET operation to verify the health of the server.

```
ip slb probe probe_name {http | https} username user_name
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
<i>user_name</i>	Specifies user name.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http username subnet1
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable  
  slbProbeName  
  slbProbeMethod  
  slbProbeHttpUsername
```

ip slb probe password

Configures a password that is sent to a server as credentials for an HTTP GET to verify the health of the server.

```
ip slb probe probe_name {http | https} password password
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
<i>password</i>	Specifies the password.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The password is encrypted in the configuration file so that it is not readable.

Examples

```
-> ip slb probe web_server http password h1f45xc
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable  
  slbProbeName  
  slbProbeMethod  
  slbProbeHttpPassword
```

ip slb probe url

Configures a URL that is sent to a server for an HTTP GET to verify the health of the server.

```
ip slb probe probe_name {http | https} url url
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
<i>url</i>	Specifies the URL of the server.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http url pub/index.html
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable  
  slbProbeName  
  slbProbeMethod  
  slbProbeHttpUrl
```

ip slb probe status

Configures the expected status returned from an HTTP GET to verify the health of a server.

```
ip slb probe probe_name {http | https} status status_value
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
<i>status_value</i>	Specifies the expected status returned.

Defaults

parameter	default
<i>status_value</i>	200

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http status 404
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable
  slbProbeName
  slbProbeMethod
  slbProbePeriod
  slbProbeHttpStatus
```

ip slb probe send

Configures an ASCII string that is sent to a server to invoke a server response and verify the health of the server.

```
ip slb probe probe_name {tcp | udp} send send_string
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
<i>send_string</i>	Specifies the ASCII string sent to a server to invoke a response.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

NA

Examples

```
-> ip slb probe web_server tcp send test
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable  
  slbProbeName  
  slbProbeMethod  
  slbProbeSend
```

ip slb probe expect

Configures an ASCII string used to compare a response from a server to verify the health of the server.

```
ip slb probe probe_name {http | https | tcp | udp} expect expect_string
```

Syntax Definitions

<i>probe_name</i>	Specifies the name of the Server Load Balancing (SLB) probe.
http	Specifies an HTTP probe.
https	Specifies an HTTPS probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.
<i>expect_string</i>	Specifies the ASCII string used to compare a response from a server.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip slb probe web_server http expect test
```

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
show ip slb probes	Displays the configuration of SLB probes.

MIB Objects

```
slbProbeTable  
  slbProbeName  
  slbProbeMethod  
  slbProbeExpect
```

show ip slb

Displays the status of Server Load Balancing on a switch.

show ip slb

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip slb
```

```
Admin status           : Enabled,  
Operational status    : In Service,  
Number of clusters    = 3
```

Output fields are described here:

output definitions

Admin status	The current administrative status of Server Load Balancing (SLB) on this switch (Enabled or Disabled).
Operational status	The current operational status of Server Load Balancing (SLB) on this switch, which is either In service (at least one SLB cluster is in service) or Out of service (all SLB clusters are out of service).
Number of clusters	The total number of Server Load Balancing (SLB) clusters on this switch.

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb clusters	Displays the status and configuration of all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.

MIB Objects

```
slbFeature  
  slbAdminStatus  
  slbOperStatus  
  slbClustersCount
```

show ip slb clusters

Displays the status and basic configuration for all Server Load Balancing (SLB) clusters on a switch. This command also displays traffic statistics for QoS policy condition clusters.

show ip slb clusters [statistics]

Syntax Definitions

statistics Displays SLB statistics for QoS policy condition clusters.

Defaults

By default, the status and basic configuration for all clusters is displayed; statistics are not shown.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **statistics** parameter to display the total number of packets that were passed to clusters because they met the QoS condition criteria configured for that cluster. The polling interval used to obtain such statistics is every 15 minutes. See the second example below.

Examples

```
-> show ip slb clusters
```

Cluster Name	VIP/COND	Admin Status	Operational Status	# Srv	% Avail
WorldWideWeb	128.241.130.204	Enabled	In Service	3	95
Intranet	128.241.130.205	Enabled	In Service	2	100
FileTransfer	128.241.130.206	Enabled	Out of Service	2	50

Output fields are described here:

output definitions

Cluster Name	The name of the SLB cluster.
VIP/COND	The virtual IP (VIP) address or the policy condition name for the SLB cluster.
Admin Status	The administrative status of the SLB cluster (Enabled or Disabled).
Operational Status	The operational status of the SLB cluster; In Service (at least one physical server is operational in the cluster) or Out of Service .
# Srv	The total number of physical servers that belong to the SLB cluster.
% Avail	The percentage of time that the physical server has been available for processing client requests. In other words, the actual ratio of up time (In Service plus Retrying) versus down time (No Answer plus Link Down). Please note that the Disabled and the initial Discovery states are not counted as down time.

```
-> show ip slb clusters statistics
```

```

Cluster Name           Admin   Operational
                      Status   Status           Count
-----+-----+-----+-----
Cluster1               Enabled In Service       4 Servers
Cluster2               Enabled In Service       4 Servers

Dst IP 101.113.113.1/255.255.255.255      4503911
Src IP 202.202.1.0/255.255.255.0          6527831
Src Port 2/49

```

output definitions

Cluster Name	The name of the SLB cluster. This field also contains the administrative and operational status for the cluster and either the VIP address or QoS policy condition value that identifies the cluster.
Admin Status	The administrative state of this physical server (Enabled or Disabled).
Operational Status	The operational state of this server. The possible states are described as follows: <ul style="list-style-type: none"> • Disabled (this server is administratively disabled). • No Answer (this server has not responded to ping requests). • Link Down (there is a bad connection to this server). • In Service (this server is used for SLB cluster client connections). • Discovery (the SLB cluster is pinging this physical server). • Retrying (the SLB cluster is making another attempt to bring up this server).
Count	The total number of physical servers that belong to the cluster, and the total number of packets serviced by the cluster.
Dst	The destination Virtual IP address assigned to the cluster.
Src	Source IP address assigned to the cluster.
Src Port	Source slot and port number of the SLB cluster.

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb reset statistics	Resets SLB statistics for all clusters.
show ip slb cluster	Displays detailed status and configuration information for a single SLB cluster.
show ip slb servers	Displays the status of all physical servers belonging to each SLB cluster on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in an SLB cluster.

MIB Objects

slbClusterTable

- slbClusterName
- slbClusterVIP
- slbClusterCondition
- slbClusterAdminStatus
- slbClusterOperStatus
- slbClusterNumberOfServers
- slbClusterNewFlows

slbStatsTable

- slbStatsClusterName
- slbStatsIndex
- slbStatsCounter

slbStatsQualTable

- slbStatsQualType
- slbStatsQualData

show ip slb cluster

Displays detailed statistics and configuration information and operational status for a single Server Load Balancing (SLB) cluster. This command also displays traffic statistics for single QoS policy condition cluster.

show ip slb cluster *name* [*statistics*]

Syntax Definitions

name Specifies the name of the SLB cluster.

statistics Displays SLB statistics for the specified cluster.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **statistics** parameter to display the total number of packets that were passed to the cluster because they met the QoS condition criteria configured for that cluster. The polling interval used to obtain such statistics is every 15 minutes. See the second example below:

Examples

```
-> show ip slb cluster Intranet
```

```
Cluster Intranet
VIP                : 128.241.130.204,
Type               : L3
Admin status       : Enabled,
Operational status : In Service,
Ping period (seconds) = 60,
Ping timeout (milliseconds) = 3000,
Ping retries       : 3,
Probe              : None,
Number of packets  : 25346,
Number of servers  : 3
  Server 128.241.130.107
    Admin status = Enabled, Operational status = In Service,
    Weight = 4, Availability (%) = 0
  Server 128.241.130.117
    Admin status = Enabled, Operational status = Discovery,
    Weight = 6, Availability (%) = 0
  Server 128.241.130.127
    Admin status = Enabled, Operational status = Discovery,
    Weight = 1, Availability (%) = 0
```

output definitions

Cluster	The name of this Server Load Balancing (SLB) cluster.
VIP	The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.
Type	The classifier for the hypothetical packet, which can be L2 or L3 .
Admin status	The current administrative status of this Server Load Balancing (SLB) cluster (Enabled or Disabled).
Operational status	The current operational status of this Server Load Balancing (SLB) cluster, which is In Service (at least one physical server is operational in the cluster) or Out of Service .
Ping period (seconds)	The ping period (in seconds) used by this Server Load Balancing (SLB) cluster to check the health of physical servers.
Ping timeout (milliseconds)	The timeout (in milliseconds) used by this Server Load Balancing (SLB) cluster to wait for ping answers from physical servers.
Ping retries	The number of ping retries that this Server Load Balancing (SLB) cluster executes before switching the status to No answer .
Probe	The probe configured for this cluster.
Number of packets	The number of packets balanced for this Server Load Balancing (SLB) cluster.
Number of servers	The total number of physical servers that belong to this Server Load Balancing (SLB) cluster.
Server	The IP address for this physical server.
Admin Status	The administrative state of this physical server (Enabled or Disabled).
Operational Status	The operational state of this server. The possible states are described as follows: <ul style="list-style-type: none"> • Disabled (this server is administratively disabled). • No Answer (this server has not responded to ping requests). • Link Down (there is a bad connection to this server). • In Service (this server is used for SLB cluster client connections). • Discovery (the SLB cluster is pinging this physical server). • Retrying (the SLB cluster is making another attempt to bring up this server).
Availability (%)	The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (In Service plus Retrying) versus down time (No Answer plus Link Down). Please note that the Disabled and the initial Discovery states are not counted as down time.

```
-> show ip slb cluster Intranet statistics
```

Cluster Name	Admin Status	Operational Status	Count
Intranet	Enabled	In Service	3 Servers
Src IP 15.2.3.2/255.255.255.255			195
Src Port 1/4			

output definitions

Cluster Name	The name of the SLB cluster. This field also contains the administrative and operational status for the cluster and either the VIP address or QoS policy condition value that identifies the cluster.
Admin status	The current administrative status of this physical server (Enabled or Disabled).
Oper status	The operational state of this server. The possible states are described as follows: <ul style="list-style-type: none"> • Disabled (this server is administratively disabled). • No Answer (this server has not responded to ping requests). • Link Down (there is a bad connection to this server). • In Service (this server is used for SLB cluster client connections). • Discovery (the SLB cluster is pinging this physical server). • Retrying (the SLB cluster is making another attempt to bring up this server).
Count	The total number of physical servers that belong to the cluster, and the total number of packets serviced by the cluster.

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb reset statistics	Resets SLB statistics for all clusters.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb cluster server	Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.
ip slb cluster probe	Configures a probe for an SLB cluster.

MIB Objects

```
slbClusterTable
  slbClusterName
  slbClusterVIP
  slbClusterAdminStatus
  slbClusterOperStatus
  slbClusterUpTime
  slbClusterPingPeriod
```

```
slbClusterPingTimeout
slbClusterPingRetries
slbClusterRedirectAlgorithm
slbClusterIdleTimer
slbClusterNumberOfServers
slbClusterProbeName
slbClusterRowStatus
slbClusterPackets
slbClusterCondition
slbClusterType
slbServerTable
  slbServerClusterName
  slbServerIpAddress
  slbServerAdminStatus
  slbServerOperStatus
slbStatsTable
  slbStatsClusterName
  slbStatsIndex
  slbStatsCounter
slbStatsQualTable
  slbStatsQualType
  slbStatsQualData
```

show ip slb cluster server

Displays detailed statistics and configuration information for a single physical server in a Server Load Balancing (SLB) cluster.

show ip slb cluster *name* **server** *ip_address*

Syntax Definitions

name Specifies the name of the Server Load Balancing (SLB) cluster.

ip_address Specifies the IP address for the physical server.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Specifying a value for the *name* and *ip_address* parameters is required.

Examples

```
-> show ip slb cluster Intranet server 128.220.40.4
Cluster c11
  VIP 128.220.40.205
  Server 128.220.40.4
    Admin status           : Enabled,
    Oper status            : In Service,
    Probe                   = phttp,
    Availability time (%)   = 95,
    Ping failures           = 0,
    Last ping round trip time (milliseconds) = 20,
    Probe status            = ,
```

Output fields are described here:

output definitions

Cluster	The name of the Server Load Balancing (SLB) cluster.
VIP	The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.
Server	The IP address for this physical server.
Admin status	The current administrative status of this physical server (Enabled or Disabled).

output definitions (continued)

Oper status	The operational state of this server. The possible states are described as follows: <ul style="list-style-type: none"> • Disabled (this server is administratively disabled). • No Answer (this server has not responded to ping requests). • Link Down (there is a bad connection to this server). • In Service (this server is used for SLB cluster client connections). • Discovery (the SLB cluster is pinging this physical server). • Retrying (the SLB cluster is making another attempt to bring up this server).
Probe	The name of the probe configured for this server.
Availability time (%)	The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (In Service plus Retrying) versus down time (No Answer plus Link Down). Please note that the Disabled and the initial Discovery states are not counted as down time.
Ping failures	The total number of pings that have failed on this physical server.
Last ping round trip time (milliseconds)	The total amount of time (in milliseconds) measured for the last valid ping to this physical server to make a round trip.
Probe status	The status of the probe configured for this server.

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb servers	Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster.

MIB Objects

slbClusterTable

slbClusterVIP

slbServerTable

slbServerClusterName

slbServerIpAddress

slbServerAdminStatus

slbServerOperStatus

slbServerMacAddress

slbServerSlotNumber

slbServerPortNumber

slbServerUpTime

slbServerProbeName

slbServerLastRTT

slbServerPingFails

 slbServerProbeStatus

show ip slb servers

Displays the status and configurations of all physical servers in Server Load Balancing clusters.

show ip slb servers

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

-> show ip slb servers

IP addr	Cluster Name	Admin Status	Operational Status	% Avail
128.220.40.4	Intranet	Enabled	In Service	98
128.220.40.5	Intranet	Enabled	Retrying	80
128.220.40.6	FileTransfer	Enabled	No answer	50
128.220.40.7	FileTransfer	Disabled	Disabled	---
128.220.40.1	WorldWideWeb	Enabled	In Service	100
128.220.40.2	WorldWideWeb	Enabled	Discovery	50
128.220.40.3	WorldWideWeb	Enabled	Link Down	75

Output fields are described here:

output definitions

IP addr	The IP address for this physical server.
Cluster Name	The name of the Server Load Balancing (SLB) cluster to which this physical server belongs.
Admin Status	The current administrative status of this physical server (Enabled or Disabled).

output definitions (continued)

Operational Status	The operational state of this server. The possible states are described as follows: <ul style="list-style-type: none">• Disabled (this server is administratively disabled).• No Answer (this server has not responded to ping requests).• Link Down (there is a bad connection to this server).• In Service (this server is used for SLB cluster client connections).• Discovery (the SLB cluster is pinging this physical server).• Retrying (the SLB cluster is making another attempt to bring up this server).
% Avail	The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (In Service plus Retrying) versus down time (No Answer plus Link Down). Please note that the Disabled and the initial Discovery states are not counted as down time.

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb cluster server	Displays the detailed status and configuration of a single physical server in a Server Load Balancing cluster.
show ip slb clusters	Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
show ip slb cluster	Displays detailed status and configuration information for a single Server Load Balancing cluster.

MIB Objects

```
slbServers
  slbServerIpAddress
  slbServerClusterName
  slbServerAdminStatus
  slbServerOperStatus
  slbServerFlows
```

show ip slb probes

Displays the configuration of Server Load Balancing (SLB) probes.

show ip slb probes [*probe_name*]

Syntax Definitions

probe_name Specifies the name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you do not specify the name of an SLB probe then all SLB probes are displayed.

Examples

No probe name is specified:

```
-> show ip slb probes
```

Probe Name	Period	Retries	Timeout	Method
web_server	60000	3	12000	HTTP
mail_server	60000	3	3000	SMTP
mis_servers	3600000	5	24000	Ping

Output fields are described here:

output definitions

Probe Name	The user-specified name of the probe.
Period	The period (in seconds) to check the health of servers.
Retries	The number of probe retries before deciding that a server is out of service.
Timeout	The timeout (in seconds) used to wait for probe answers.
Method	The type of probe.

The name of a probe that is not an HTTP/HTTPS probe is specified:

```
-> show ip slb probes mail_server
```

```
Probe mail_server
  Type                = SMTP,
  Period (seconds)    = 60,
  Timeout (milliseconds) = 3000,
  Retries              = 3,
  Port                = 0,
```

The name of an HTTP/HTTPS probe is specified:

```
-> show ip slb probes phttp
```

```
Probe phttp
  Type                = HTTP,
  Period (seconds)    = 60,
  Timeout (milliseconds) = 3000,
  Retries              = 3,
  Port                = 0,
  Username            = ,
  Password            = ,
  Expect              = ,
  Status              = 200,
  URL                 = /,
```

Output fields are described here:

output definitions

Probe	The user-specified name of the probe.
Type	The type of probe.
Period	The period (in seconds) to check the health of servers.
Timeout	The timeout (in seconds) used to wait for probe answers.
Retries	The number of probe retries before deciding that a server is out of service.
Port	The TCP/UDP port on which the probe is sent.
Username	The configured user name sent to a server as credentials for an HTTP GET operation for the probe.
Password	The configured password for the probe.
Expect	The configured ASCII string used to compare a response from a server to verify the health of the server.
Status	The expected status returned from an HTTP GET to verify the health of a server.
URL	The configured URL sent to a server for an HTTP GET to verify the health of the server.

Release History

Release 7.1.1; command introduced.

Related Commands

ip slb probe	Configures and deletes SLB probes.
ip slb probe period	Configures the probe period to check the health of servers.
ip slb probe timeout	Configures the timeout used to wait for probe answers.
ip slb probe retries	Configures the number of probe retries before deciding that a server is out of service.
ip slb probe port	Configures the TCP/UDP port that the probe should be sent on.
ip slb probe username	Configures a user name sent to a server as credentials for an HTTP GET operation
ip slb probe password	Configures a password sent to a server as credentials for an HTTP GET to verify the health of the server
ip slb probe expect	Configures an ASCII string used to compare a response from a server to verify the health of the server.
ip slb probe status	Configures the expected status returned from an HTTP GET to verify the health of a server.
ip slb probe url	Configures a URL sent to a server for an HTTP GET to verify the health of the server.

MIB Objects

```
slbProbeTable
  slbProbeName
  slbProbeMethod
  slbProbePeriod
  slbProbeTimeout
  slbProbeRetries
  slbProbePort
  slbProbeHttpUsername
  slbProbeHttpPassword
  slbProbeExpect
  slbProbeHttpStatus
  slbProbeHttpUrl
```

24 IP Multicast Switching Commands

IP Multicast Switching (IPMS) is a one-to-many communication technique employed by emerging applications such as video distribution, news feeds, conferencing, netcasting, and resource discovery (OSPF, RIP2, and BOOTP). Unlike unicast, which sends one packet per destination, multicast sends one packet to all devices in any subnetwork that has at least one device requesting the multicast traffic.

Alcatel-Lucent's IPMS software is compatible with the following RFCs:

- RFC 1112 — Host Extensions for IP Multicasting
- RFC 2236 — Internet Group Management Protocol, Version 2
- RFC 2933 — Internet Group Management Protocol MIB
- RFC 3376 — Internet Group Management Protocol, Version 3

Alcatel-Lucent's IPv6MS software is compatible with the following RFCs:

- RFC 2710 — Multicast Listener Discovery for IPv6
- RFC 3019 — IPv6 MIB for Multicast Listener Discovery Protocol
- RFC 3810 — Multicast Listener Discovery Version 2 for IPv6

MIB information for the IPMS commands is as follows:

Filename: AlcatelIND1Igmp.mib
Module: ALCATEL-IGMP-IND1-MIB

MIB information for the IPv6MS commands is as follows:

Filename: AlcatelIND1Mld.mib
Module: ALCATEL-MLD-IND1-MIB

The following table summarizes the available IP and IPv6 multicast commands:

ip multicast admin-state
ip multicast querier-forwarding
ip multicast version
ip multicast max-group
ip multicast vlan max-group
ip multicast port max-group
ip multicast static-querier
ip multicast static-group
ip multicast query-interval
ip multicast last-member-query-interval
ip multicast query-response-interval
ip multicast unsolicited-report-interval
ip multicast router-timeout
ip multicast source-timeout
ip multicast querying
ip multicast robustness
ip multicast spoofing
ip multicast zapping
ip multicast proxying
ip multicast helper-address
ipv6 multicast admin-state
ipv6 multicast querier-forwarding
ipv6 multicast version
ipv6 multicast max-group
ipv6 multicast vlan max-group
ipv6 multicast port max-group
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 neighbor
show ip multicast querier
show ip multicast group
show ip multicast source
show ip multicast tunnel
show ipv6 multicast
show ipv6 multicast port
show ipv6 multicast neighbor
show ipv6 multicast querier
show ipv6 multicast group
show ipv6 multicast source
show ipv6 multicast tunnel

ip multicast admin-state

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*] **admin-state** [{**enable** | **disable**}]

Syntax Definitions

<i>vid</i>	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 10K, 6900

Usage Guidelines

- If an IP Multicast Routing protocol is already running on the system, the **ip multicast admin-state** 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 admin-state**.
- 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* admin-state**.

Examples

```
-> ip multicast admin-state enable
-> ip multicast admin-state disable
-> ip multicast vlan 2 admin-state enable
-> ip multicast vlan 2 admin-state disable
-> ip multicast vlan 2 admin-state
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmp

 alaIcmpStatus

alaIcmpVlan

 alaIcmpVlanStatus

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

<i>vid</i>	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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmp
  alaIcmpQuerierForwarding
alaIcmpVlan
  alaIcmpVlanQuerierForwarding
```

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
<i>version</i>	2

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmp
  alaIcmpVersion
alaIcmpVlan
  alaIcmpVlanVersion
```

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

<i>num</i>	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 10K, 6900

Usage Guidelines

- Configuring a max-group value will have no effect 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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmpMaxGroupLimit  
alaIcmpMaxGroupExceedAction
```

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

<i>vid</i>	VLAN on which to apply the configuration.
<i>num</i>	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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmpVlanTable

 alaIcmpVlanMaxGroupLimit

 alaIcmpVlanMaxGroupExceedAction

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

<i>slot / port</i>	The slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3).
<i>num</i>	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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmpPortTable

 alaIcmpPortMaxGroupLimit

 alaIcmpPortMaxGroupExceedAction

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* | **linkagg** *linkagg*}

no ip multicast static-neighbor vlan *vid* {**port** *slot/port* | **linkagg** *linkagg*}

Syntax Definitions

<i>vid</i>	VLAN to include as a static IGMP neighbor.
<i>slot/port</i>	The slot/port number you want to configure as a static IGMP neighbor.
<i>linkagg</i>	The link aggregate identifier you want to configure as a static IGMP neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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* **linkagg**, followed by the link aggregation group number (e.g., `ip multicast static-neighbor vlan 2 linkagg 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 7.1.1; command was introduced.

Release 7.3.1; **linkagg** parameter was introduced.

Related Commands

show ip multicast neighbor Displays the IGMP neighbor table entries of IP Multicast Switching and Routing.

MIB Objects

```
alaIcmpStaticNeighborTable  
  alaIcmpStaticNeighborVlan  
  alaIcmpStaticNeighborIfIndex  
  alaIcmpStaticNeighborRowStatus
```

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* / **linkagg** *linkagg*}

no ip multicast static-querier vlan *vid* {**port** *slot/port* / **linkagg** *linkagg*}

Syntax Definitions

<i>vid</i>	VLAN to include as a static IGMP querier.
<i>slot/port</i>	The slot/port number you want to configure as a static IGMP querier.
<i>linkagg</i>	The link aggregate id number to configure as a static IGMP querier.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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* **linkagg**, followed by the link aggregation group number (e.g., `ip multicast static-querier vlan 2 linkagg 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 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.

Related Commands

show ip multicast querier

Displays the IGMP querier table entries of IP Multicast Switching and Routing.

MIB Objects

```
alaIgmStaticQuerierTable  
  alaIgmStaticQuerierVlan  
  alaIgmStaticQuerierIfIndex  
  alaIgmStaticQuerierRowStatus
```

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* / **linkagg** *linkagg*}

no ip multicast static-group *ip_address* **vlan** *vid* {**port** *slot/port* / **linkagg** *linkagg*}

Syntax Definitions

<i>ip_address</i>	The IP address of the multicast group.
<i>vid</i>	VLAN to include as a static IGMP group.
<i>slot/port</i>	The slot/port number you want to configure as a static IGMP group.
<i>linkagg</i>	The link aggregate identifier you want to configure as a static IGMP group.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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* **linkagg**, followed by the link aggregation group number (e.g., `ip multicast static-group 225.0.0.1 vlan 2 linkagg 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
-> no ip multicast static-group 225.11.11.11 vlan 4 port 7
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.

Related Commands

show ip multicast group

Displays the IGMP group membership table entries of IP Multicast Switching and Routing for the specified IP multicast group address or all entries if no IP multicast group address is specified.

MIB Objects

```
alaIcmpStaticMemberTable  
  alaIcmpStaticMemberVlan  
  alaIcmpStaticMemberIfIndex  
  alaIcmpStaticMemberGroupAddress  
  alaIcmpStaticMemberRowStatus
```

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
<i>seconds</i>	125

Platforms Supported

OmniSwitch 10K, 6900

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 (i.e., 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 (i.e., 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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmp
  alaIcmpQueryInterval
alaIcmpVlan
  alaIcmpVlanQueryInterval
```

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

<i>vid</i>	VLAN on which to apply the configuration.
<i>tenths-of-seconds</i>	IGMP last member query interval in tenths of seconds. Valid range is 1 to 65535.

Defaults

parameter	default
<i>tenths-of-seconds</i>	10

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show ip multicast](#)

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmp

 alaIcmpLastMemberQueryInterval

alaIcmpVlan

 alaIcmpVlanLastMemberQueryInterval

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

<i>vid</i>	VLAN on which to apply the configuration.
<i>tenths-of-seconds</i>	IGMP query response interval in tenths of seconds. Valid range is 1 to 65535.

Defaults

parameter	default
<i>tenths-of-seconds</i>	100

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show ip multicast](#)

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmp

 alaIcmpQueryResponseInterval

alaIcmpVlan

 alaIcmpVlanQueryResponseInterval

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

<i>vid</i>	VLAN on which to apply the configuration.
<i>seconds</i>	IGMP query response interval in seconds. Valid range is 1 to 65535, where 0 represents the default setting.

Defaults

parameter	default
<i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show ip multicast](#)

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmp

 alaIcmpUnsolicitedReportInterval

alaIcmpVlan

 alaIcmpVlanUnsolicitedReportInterval

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
<i>seconds</i>	90

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmp
  alaIcmpRouterTimeout
alaIcmpVlan
  alaIcmpVlanRouterTimeout
```

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
<i>seconds</i>	30

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmp
  alaIcmpSourceTimeout
alaIcmpVlan
  alaIcmpVlanSourceTimeout
```

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

<i>vid</i>	VLAN on which configuration is applied.
enable	Enable IGMP querying.
disable	Disable IGMP querying.

Defaults

parameter	default
enable / disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmp

 alaIcmpQuerying

alaIcmpVlan

 alaIcmpVlanQuerying

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
<i>robustness</i>	2

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmp
  alaIcmpRobustness
alaIcmpVlan
  alaIcmpVlanRobustness
```

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

<i>vid</i>	VLAN on which to apply the configuration.
enable	Enable IGMP spoofing.
disable	Disable IGMP spoofing.

Defaults

parameter	default
enable / disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show ip multicast](#)

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmp

 alaIcmpSpoofing

alaIcmpVlan

 alaIcmpVlanSpoofing

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

<i>vid</i>	VLAN on which to apply the configuration.
enable	Enable IGMP zapping.
disable	Disable IGMP zapping.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmp
  alaIcmpZapping
alaIcmpVlan
  alaIcmpVlanZapping
```

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

<i>vid</i>	VLAN on which to apply the configuration.
enable	Enable IGMP proxying.
disable	Disable IGMP proxying.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIcmp
  alaIcmpProxying
alaIcmpVlan
  alaIcmpVlanProxying
```

ip multicast helper-address

Specifies the destination IP address of a relay host where IGMP host reports and Leave messages are to be sent.

ip multicast helper-address [*ip-address*]

Syntax Definitions

ip-address The IP address of the relay host

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- After the destination IP address is specified, the IPMS reporting feature is enabled.
- To disable the IPMS reporting feature, 0.0.0.0 is used as the IP address. It can also be disabled by omitting the IP address from the command.

Examples

```
-> ip multicast helper-address 10.1.1.198
-> ip multicast helper-address 0.0.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip multicast](#) Displays the IP Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaIgmp
  alaIgmpHelperAddress
  alaIgmpHelperAddressType
```

ipv6 multicast admin-state

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*] admin-state [{enable | disable}]

Syntax Definitions

<i>vid</i>	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 10K, 6900

Usage Guidelines

- If an IPv6 multicast routing protocol is already running on the system, this 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 this command.
- You can also restore the MLD querying to its default (i.e., disabled) status on the specified VLAN, by using this command.

Examples

```
-> ipv6 multicast admin-state enable
-> ipv6 multicast admin-state disable
-> ipv6 multicast admin-state
-> ipv6 multicast vlan 2 admin-state enable
-> ipv6 multicast vlan 2 admin-state disable
-> ipv6 multicast vlan 2 admin-state
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  alaMldStatus
alaMldVlan
  alaMldVlanStatus
```

ipv6 multicast querier-forwarding

Enables or disables MLD querier forwarding on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid*] querier-forwarding [{enable | disable}]

no ipv6 multicast [vlan *vid*] querier-forwarding

Syntax Definitions

<i>vid</i>	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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

`show ipv6 multicast`

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  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
<i>version</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  alaMldVersion
alaMldVlan
  alaMldVlanVersion
```

ipv6 multicast max-group

Configures the global maximum group limit that can be learned per port/VLAN instance. The limit is applied to each port/VLAN instance and an action is taken when it exceeds the limit.

ipv6 multicast max-group [*num*] [**action** {**none** | **drop** | **replace**}]

Syntax Definitions

<i>num</i>	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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaIcmpMaxGroupLimit
alaIcmpMaxGroupExceedAction

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

<i>vid</i>	VLAN on which to apply the configuration.
<i>num</i>	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 10K, 6900

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 7.1.1; 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

alaIcmpVlanTable

 alaIcmpVlanMaxGroupLimit

 alaIcmpVlanMaxGroupExceedAction

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

<i>slot / port</i>	The slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3).
<i>num</i>	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 10K, 6900

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 7.1.1; 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

alaIcmpPortTable

 alaIcmpPortMaxGroupLimit

 alaIcmpPortMaxGroupExceedAction

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** | **linkagg linkagg**}

no ipv6 multicast static-neighbor *vlan vid* {**port slot/port** | **linkagg linkagg**}

Syntax Definitions

<i>vid</i>	VLAN to include as a static MLD neighbor.
<i>slot/port</i>	The slot/port number you want to configure as a static MLD neighbor.
<i>linkagg</i>	The link aggregate you want to configure as a static MLD neighbor.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 linkagg*, followed by the link aggregation group number (e.g., `ipv6 multicast static-neighbor vlan 2 linkagg 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 7.1.1; command was introduced.

Release 7.3.1; **linkagg** parameter was added.

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** | **linkagg linkagg**}

no ipv6 multicast static-querier *vlan vid* {**port slot/port** | **linkagg linkagg**}

Syntax Definitions

<i>vid</i>	VLAN to include as a static MLD querier.
<i>slot/port</i>	The slot/port number you want to configure as a static MLD querier.
<i>linkagg</i>	The link aggregate you want to configure as a static MLD querier.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 linkagg*, followed by the link aggregation group number (e.g., `ipv6 multicast static-querier vlan 2 linkagg 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 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.

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 | linkagg linkagg}
```

```
no ipv6 multicast static-group ip_address vlan vid {port slot/port | linkagg linkagg}
```

Syntax Definitions

<i>ip_address</i>	IPv6 multicast group address.
<i>vid</i>	VLAN to include as a static MLD group.
<i>slot/port</i>	The slot/port number you want to configure as a static MLD group.
<i>linkagg</i>	The link aggregate you want to configure as a static MLD group.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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* **linkagg****, followed by the link aggregation group number (e.g., `ipv6 multicast static-group ff05::5 vlan 2 linkagg 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 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was added.

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
<i>seconds</i>	125

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

`show ipv6 multicast`

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  alaMldQueryInterval
alaMldVlan
  alaMldVlanQueryInterval
```

ipv6 multicast last-member-query-interval

Sets the MLD last member query interval on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid*] last-member-query-interval [*milliseconds*]

Syntax Definitions

<i>vid</i>	VLAN on which to apply the configuration.
<i>milliseconds</i>	MLD last member query interval in milliseconds. Valid range is 1 to 65535.

Defaults

parameter	default
<i>milliseconds</i>	1000

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show ipv6 multicast](#)

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaMld

 alaMldLastMemberQueryInterval

alaMldVlan

 alaMldVlanLastMemberQueryInterval

ipv6 multicast query-response-interval

Sets the MLD query response interval on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [*vlan vid*] **query-response-interval** [*milliseconds*]

Syntax Definitions

vid VLAN on which to apply the configuration.

milliseconds MLD query response interval in milliseconds. Valid range is 1 to 65535.

Defaults

parameter	default
<i>milliseconds</i>	10000

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaMld

 alaMldQueryResponseInterval

alaMldVlan

 alaMldVlanQueryReponseInterval

ipv6 multicast unsolicited-report-interval

Sets the MLD unsolicited report interval on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [*vlan vid*] **unsolicited-report-interval** [*seconds*]

Syntax Definitions

<i>vid</i>	VLAN on which to apply the configuration.
<i>seconds</i>	MLD unsolicited report interval in seconds. Valid range is 1 to 65535, where 0 represents the default setting.

Defaults

parameter	default
<i>seconds</i>	1

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show ipv6 multicast](#)

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaMld

 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
<i>seconds</i>	90

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  alaMldRouterTimeout
alaMldVlan
  alaMldVlanRouterTimeout
```

ipv6 multicast source-timeout

Configures the expiry time of IPv6 multicast sources on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [*vlan vid*] **source-timeout** [*seconds*]

Syntax Definitions

vid VLAN on which to apply the configuration.

seconds MLD source timeout in seconds. Valid range is 1 to 65535.

Defaults

parameter	default
<i>seconds</i>	30

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  alaMldSourceTimeout
alaMldVlan
  alaMldVlanSourceTimeout
```

ipv6 multicast querying

Enables or disables MLD querying on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid*] querying [{enable | disable}]

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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show ipv6 multicast](#)

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

alaMld

 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
<i>robustness</i>	2

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  alaMldRobustness
alaMldVlan
  alaMldVlanRobustness
```

ipv6 multicast spoofing

Enables or disables MLD spoofing on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid*] spoofing [{enable | disable}]

no ipv6 multicast [vlan *vid*] spoofing

Syntax Definitions

<i>vid</i>	VLAN on which to apply the configuration.
enable	Enable MLD spoofing.
disable	Disable MLD spoofing.

Defaults

parameter	defaults
enable / disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  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

<i>vid</i>	VLAN on which to apply the configuration.
enable	Enable MLD zapping.
disable	Disable MLD zapping.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  alaMldZapping
alaMldVlan
  alaMldVlanZapping
```

ipv6 multicast proxying

Enables or disables MLD proxying on the specified VLAN or on the system if no VLAN is specified.

ipv6 multicast [vlan *vid*] proxying [enable | disable]

Syntax Definitions

<i>vid</i>	VLAN on which to apply the configuration.
enable	Enable MLD proxying.
disable	Disable MLD proxying.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN or on the system if no VLAN is specified.

MIB Objects

```
alaMld
  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 10K, 6900

Usage Guidelines

Specify a VLAN ID to display the configuration information for an individual VLAN.

Examples

```
-> show ip multicast
```

```
Status: Enabled
Querying: Disabled
Proxying Disabled
Spoofing: Disabled
Zapping: Disabled
Querier Forwarding: Disabled
Version: 2
Robustness: 2
Query Interval (seconds): 125
Query Response Interval (tenths of seconds): 100
Last Member Query Interval(tenths of seconds):10
Unsolicited Report Interval(seconds): 1
Router Timeout (seconds): 90
Source Timeout (seconds): 30
```

```
-> show ip multicast vlan 1
```

```
Status:                               Enabled
Querying:                             Disabled
Proxying:                             Disabled
Spoofing:                             Disabled
Zapping:                              Disabled
Querier Forwarding:                   Disabled
Version:                               2
Robustness:                           2
Query Interval (seconds):              125
Query Response Interval (tenths of seconds): 100
Last Member Query Interval(tenths of seconds):10
Unsolicited Report Interval(seconds):  1
Router Timeout (seconds):              90
Source Timeout (seconds):              30
```

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 admin-state command, which is described on page 24-3 .
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 24-33 .
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 24-41 .
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 24-37 .
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 24-39 .
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 24-5 .
Version	Displays the default IGMP version, which can be 1 , 2 or 3 . Use the ip multicast version command to modify this parameter.
Robustness	Displays the IGMP robustness value, ranging from 1 to 7 . (The default value is 2). Use the ip multicast robustness command to modify this parameter.

output definitions

Query Interval (seconds)	Displays the time (in seconds) between IGMP queries. (The default value is 125 seconds). You can modify this parameter with the ip multicast query-interval command, which is described on page 24-21 .
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 24-25 .
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 24-23 .
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 24-27 .
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 24-29 .
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 24-31 .

Release History

Release 7.1.1; command was introduced.

Related Commands

ip multicast admin-state	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

```

alaIgmP
  alaIgmPStatus
  alaIgmPQuerying
  alaIgmPProxying
  alaIgmPSpoofing
  alaIgmPZapping
  alaIgmPQuerierForwarding
  alaIgmPVersion
  alaIgmPRobustness
  alaIgmPQueryInterval
  alaIgmPQueryResponseInterval
  alaIgmPLastMemberQueryInterval
  alaIgmPUnsolicitedReportInterval
  alaIgmPRouterTimeout
  alaIgmPSourceTimeout
alaIgmPVlan
  alaIgmPVlanStatus
  alaIgmPVlanQuerying
  alaIgmPVlanProxying

```

```
alaIcmpVlanSpoofing  
alaIcmpVlanZapping  
alaIcmpVlanQuerierForwarding  
alaIcmpVlanVersion  
alaIcmpVlanRobustness  
alaIcmpVlanQueryInterval  
alaIcmpVlanQueryResponseInterval  
alaIcmpVlanLastMemberQueryInterval  
alaIcmpVlanUnsolicitedReportInterval  
alaIcmpVlanRouterTimeout  
alaIcmpVlanSourceTimeout
```

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 10K, 6900

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 Groups	Max-group	Action
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 group	max-group	action
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 7.1.1; command was introduced.

Related Commands

ip multicast admin-state	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

alaIcmpPortTable

- alaIcmpPortMaxGroupLimit
- alaIcmpPortMaxGroupExceedAction

alaIcmpPortVlanTable

- alaIcmpPortVlanCurrentGroupCount
- alaIcmpPortVlanMaxGroupLimit
- alaIcmpPortVlanMaxGroupExceedAction

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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip multicast forward
```

```
Total 1 Forwards
```

Group Address	Host Address	Tunnel Address	Ingress		Egress	
			VLAN	Port	VLAN	Port
228.0.0.1	1.0.0.2	0.0.0.0	1	2/1	1	2/23

```
-> show ip multicast forward 228.0.0.1
```

Group Address	Host Address	Tunnel Address	Ingress		Egress	
			VLAN	Port	VLAN	Port
228.0.0.1	1.0.0.2	0.0.0.0	1	2/1	1	2/23

Output fields are described here:

output definitions

Group Address	IP group address of the IP multicast forward.
Host Address	IP host address of the IP multicast forward.
Tunnel Address	IP source tunnel address of the IP multicast forward.
VLAN	VLAN associated with the IP multicast forward.
Port	The slot and port number of the IP multicast forward.

Release History

Release 7.1.1; 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

```
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 10K, 6900

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 7.1.1; 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

```
alaIcmpNeighborTable
  alaIcmpNeighborVlan
  alaIcmpNeighborIfIndex
  alaIcmpNeighborHostAddress
  alaIcmpNeighborCount
  alaIcmpNeighborTimeout
  alaIcmpNeighborUpTime
alaIcmpStaticNeighborTable
  alaIcmpStaticNeighborVlan
  alaIcmpStaticNeighborIfIndex
  alaIcmpStaticNeighborRowStatus
```

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 10K, 6900

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 7.1.1; 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

```
alaIcmpQuerierTable
  alaIcmpQuerierVlan
  alaIcmpQuerierIfIndex
  alaIcmpQuerierHostAddress
  alaIcmpQuerierCount
  alaIcmpQuerierTimeout
  alaIcmpQuerierUpTime
alaIcmpStaticQuerierTable
  alaIcmpStaticQuerierVlan
  alaIcmpStaticQuerierIfIndex
  alaIcmpStaticQuerierRowStatus
```

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 10K, 6900

Usage Guidelines

N/A

Examples

-> show ip multicast group

```
Total 3 Groups
Group Address    Source Address  VLAN  Port  Mode    Static  Count  Life
-----+-----+-----+-----+-----+-----+-----+-----
231.0.0.3       1.0.0.5        1     2/1  exclude no       1     257
234.0.0.4       0.0.0.0        1     2/1  exclude no       1     218
229.0.0.1       0.0.0.0        1     2/13 exclude yes    0      0
```

-> show ip multicast group 234.0.0.4

```
Group Address    Source Address  VLAN  Port  Mode    Static  Count  Life
-----+-----+-----+-----+-----+-----+-----+-----
234.0.0.4       0.0.0.0        1     2/1  exclude no       1     218
```

Output fields are described here:

output definitions

Group Address	IP address of the IP multicast group.
Source Address	IP address of the IP multicast source.
VLAN	The VLAN associated with the IP multicast group.
Port	The slot and port number of the IP multicast group.
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.

Release History

Release 7.1.1; 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 10K, 6900

Usage Guidelines

N/A

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 228.0.0.1
```

```
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
```

output definitions

Group Address	IP group address of the IP multicast source.
Host Address	IP host address of the IP multicast source.
Tunnel Address	IP destination tunnel address of the IP multicast source.
VLAN	VLAN associated with the IP multicast source.
Port	The slot and port number of the IP multicast source.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip multicast tunnel](#)

Display the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

MIB Objects

```
alaIcmpSourceTable  
  alaIcmpSourceVlan  
  alaIcmpSourceIfIndex  
  alaIcmpSourceGroupAddress  
  alaIcmpSourceHostAddress  
  alaIcmpSourceDestAddress  
  alaIcmpSourceOrigAddress  
  alaIcmpSourceType  
  alaIcmpSourceUpTime
```

show ip multicast tunnel

Display the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

show ip multicast tunnel [address]

Syntax Definitions

address IP multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip multicast tunnel
Total 1 Tunnels
```

Group Address	Host Address	Tunnel Address	Ingress	
			VLAN	Port
228.0.0.1	1.0.0.2	2.1.2.3	1	2/1

output definitions

Group Address	IP group address of the IP multicast tunnel.
Host Address	IP host address of the IP multicast tunnel.
Tunnel Address	IP source tunnel address of the IP multicast tunnel.
VLAN	VLAN associated with the IP multicast tunnel.
Port	The slot and port number of the IP multicast tunnel.

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

```
alaIcmpTunnelTable  
  alaIcmpTunnelVlan  
  alaIcmpTunnelIfIndex  
  alaIcmpTunnelGroupAddress  
  alaIcmpTunnelHostAddress  
  alaIcmpTunnelDestAddress  
  alaIcmpTunnelOrigAddress  
  alaIcmpTunnelType  
  alaIcmpTunnelNextDestAddress  
  alaIcmpTunnelNextType
```

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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast
```

```
Status: = Enabled
Querying: = Disabled
Proxying: = Disabled
Spoofing: = Disabled
Zapping: = Disabled
Querier Forwarding: = Disabled
Version: = 1
Robustness: = 2
Query Interval (seconds): = 125
Query Response Interval (milliseconds): = 10000
Last Member Query Interval (milliseconds): = 1000
Unsolicited Report Interval (seconds) = 1,
Router Timeout (seconds): = 90
Source Timeout (seconds): = 30
```

```
-> show ipv6 multicast vlan 1
```

```
Status:                               = Enabled
Querying:                              = Disabled
Proxying:                               = Disabled
Spoofing:                              = Disabled
Zapping:                                = Disabled
Querier Forwarding:                    = Disabled
Version:                                = 1
Robustness:                             = 2
Query Interval (seconds):               = 125
Query Response Interval (milliseconds): = 10000
Last Member Query Interval (milliseconds): = 1000
Unsolicited Report Interval (seconds)   = 1,
Router Timeout (seconds):               = 90
Source Timeout (seconds):               = 30:
```

output definitions

Status	Whether the IPv6 Multicast Switching and Routing is Enabled or Disabled (the default status). You can enable or disable IPv6 Multicast Switching and Routing with the ip multicast helper-address command, which is described on page 24-43
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 24-74
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 24-82
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 24-37
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 24-80
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 24-46 .
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 24-62 .

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 24-66 .
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 24-64 .
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 24-68 .
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 24-70
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 24-72

Release History

Release 7.1.1; command was introduced.

Related Commands

ip multicast helper-address	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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

ipv6 multicast admin-state	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 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.
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.

MIB Objects

```

alaIcmpPortTable
  alaIcmpPortMaxGroupLimit
  alaIcmpPortMaxGroupExceedAction
alaIcmpPortVlanTable
  alaIcmpPortVlanCurrentGroupCount
  alaIcmpPortVlanMaxGroupLimit
  alaIcmpPortVlanMaxGroupExceedAction

```


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_address*]

Syntax Definitions

ipv6_address IPv6 multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast forward
```

```
Total 1 Forwards
```

Group Address	Host Address	Tunnel Address	Ingress		Egress	
			VLAN	Port	VLAN	Port
ff05::6	4444::2	::	1	2/1	1	2/23

```
-> show ipv6 multicast forward ff05::6
```

Group Address	Host Address	Tunnel Address	Ingress		Egress	
			VLAN	Port	VLAN	Port
ff05::6	4444::2	::	1	2/1	1	2/23

output definitions

Group Address	IPv6 group address of the IPv6 multicast forward.
Host Address	IPv6 host address of the IPv6 multicast forward.
Tunnel Address	IPv6 source tunnel address of the IPv6 multicast forward.
VLAN	VLAN associated with the IPv6 multicast forward.
Port	The slot and port number of the IPv6 multicast forward.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 multicast static-group Creates a static MLD group entry on a specified port on a specified VLAN.

MIB Objects

```
alaMldForwardTable
  alaMldForwardVlan
  alaMldForwardIfIndex
  alaMldForwardGroupAddress
  alaMldForwardHostAddress
  alaMldForwardDestAddress
  alaMldForwardOrigAddress
  alaMldForwardType
  alaMldForwardNextVlan
  alaMldForwardNextIfIndex
  alaMldForwardNextDestAddress
  alaMldForwardNextType
  alaMldForwardTtl
```

show ipv6 multicast neighbor

Displays the MLD neighbor table entries of IPv6 Multicast Switching and Routing.

show ipv6 multicast neighbor

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

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 7.1.1; command was introduced

Related Commands

ipv6 multicast static-querier Creates a static MLD querier entry on a specified port on a specified VLAN.

MIB Objects

```
alaMldQuerierTable
  alaMldQuerierVlan
  alaMldQuerierIfIndex
  alaMldQuerierHostAddress
  alaMldQuerierCount
  alaMldQuerierTimeout
  alaMldQuerierUpTime
alaMldStaticQuerierTable
  alaMldStaticQuerierVlan
  alaMldStaticQuerierIfIndex
  alaMldStaticQuerierRowStatus
```

show ipv6 multicast group

Displays the MLD group membership table entries of IPv6 Multicast Switching and Routing for the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

show ipv6 multicast group [*ip_address*]

Syntax Definitions

ip_address IPv6 multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced

Related Commands

ipv6 multicast static-group Creates a static MLD group entry on a specified port on a specified VLAN.

MIB Objects

```
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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast source
```

```
Total 1 Sources
Group Address   Host Address   Tunnel Address  VLAN  Port
-----+-----+-----+-----+-----
ff05::6        4444::2       ::             1     2/1
```

```
-> show ipv6 multicast source ff05::6
```

```
Total 1 Sources
Group Address   Host Address   Tunnel Address  VLAN  Port
-----+-----+-----+-----+-----
ff05::6        4444::2       ::             1     2/1
```

output definitions

Group Address	IPv6 group address of the IPv6 multicast source.
Host Address	IPv6 host address of the IPv6 multicast source.
Tunnel Address	IPv6 source tunnel address of the IPv6 multicast source.
VLAN	VLAN associated with the IPv6 multicast source.
Port	The slot and port number of the IPv6 multicast source.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 multicast static-group

Creates a static MLD group entry on a specified port on a specified VLAN.

MIB Objects

```
alaMldSourceTable  
  alaMldSourceVlan  
  alaMldSourceIfIndex  
  alaMldSourceGroupAddress  
  alaMldSourceHostAddress  
  alaMldSourceDestAddress  
  alaMldSourceOrigAddress  
  alaMldSourceType  
  alaMldSourceUpTime
```

show ipv6 multicast tunnel

Displays the IPv6 Multicast Switching and Routing tunneling table entries matching the specified IPv6 multicast group address, or all entries if no IPv6 multicast address is specified.

show ipv6 multicast tunnel [*address*]

Syntax Definitions

address IPv6 multicast group address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 multicast tunnel
Total 1 Tunnels
```

Group Address	Host Address	Tunnel Address	Ingress	
			VLAN	Port
ff05::6	4444::2	3333::2	1	2/1

output definitions

Group Address	IPv6 group address of the IPv6 multicast tunnel.
Host Address	IPv6 host address of the IPv6 multicast tunnel.
Tunnel Address	IPv6 source tunnel address of the IPv6 multicast tunnel.
VLAN	VLAN associated with the IPv6 multicast tunnel.
Port	The slot and port number of the IPv6 multicast tunnel.

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

```
alaMldTunnelTable  
  alaMldTunnelVlan  
  alaMldTunnelIfIndex  
  alaMldTunnelGroupAddress  
  alaMldTunnelHostAddress  
  alaMldTunnelDestAddress  
  alaMldTunnelOrigAddress  
  alaMldTunnelType  
  alaMldTunnelNextDestAddress  
  alaMldTunnelNextType
```

25 DVMRP Commands

This chapter includes CLI command descriptions for Distance Vector Multicast Routing Protocol (DVMRP), version 3.

DVMRPv3 is a dense-mode multicast routing protocol that enables routers to efficiently propagate IP multicast traffic through a network. Multicast traffic consists of a data stream that originates from a single source and is sent to hosts that have subscribed to that stream. Live video broadcasts, video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news services are examples of multicast traffic.

For more information about configuring DVMRP, see the applicable *OmniSwitch Advanced Routing Configuration Guide*.

MIB information for the DVMRP commands is as follows:

Filename: AlcatelIND1Dvmrp.MIB
Module: ALCATEL-IND1-DVMRP-MIB

Filename: IETF_DVMRP_STD_DRAFT.MIB
Module: DVMRP-STD-MIB

A summary of the available commands is listed here:

ip load dvmrp
ip dvmrp admin-state
ip dvmrp flash-interval
ip dvmrp graft-timeout
ip dvmrp interface
ip dvmrp interface metric
ip dvmrp neighbor-interval
ip dvmrp neighbor-timeout
ip dvmrp prune-lifetime
ip dvmrp prune-timeout
ip dvmrp report-interval
ip dvmrp route-holddown
ip dvmrp route-timeout
ip dvmrp subord-default
ip interface tunnel
show ip dvmrp
show ip dvmrp
show ip dvmrp
show ip dvmrp interface
show ip dvmrp neighbor
show ip dvmrp nexthop
show ip dvmrp prune
show ip dvmrp route
show ip dvmrp tunnel

ip load dvmrp

Dynamically loads DVMRP to memory.

ip load dvmrp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command must be executed before DVMRP can be configured on the switch. In addition, DVMRP must be administratively enabled before you can run the protocol on the switch. For more information, refer to the [ip dvmrp admin-state command on page 25-3](#).

Examples

```
-> ip load dvmrp
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip dvmrp admin-state](#) Globally enables or disables DVMRP protocol on the switch.

MIB Objects

```
alaDrcTmConfig  
  alaDrcTmIPDvmrpStatus
```

ip dvmrp admin-state

Globally enables or disables DVMRP protocol on the switch.

ip dvmrp admin-state {enable | disable}

Syntax Definitions

enable	Administratively enables DVMRP on the switch.
disable	Administratively disables DVMRP on the switch.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command must be set to **enable** before DVMRP can run on the switch. In addition, the **ip load dvmrp** command must be issued. For more information, refer to the [ip load dvmrp command on page 25-2](#).
- To enable or disable DVMRP for a particular interface, refer to the [ip dvmrp interface command on page 25-6](#).

Examples

```
-> ip dvmrp admin-state enable
-> ip dvmrp admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp interface	Enables or disables the DVMRP protocol on a specified interface.
ip load dvmrp	Dynamically loads DVMRP to memory.
show ip dvmrp	Displays global DVMRP parameters, including current status.

MIB Objects

```
alaDvmrpGlobalConfig
  alaDvmrpAdminStatus
```

ip dvmrp flash-interval

Configures the minimum flash update interval value. The flash update interval defines how often routing table change messages are sent to neighboring DVMRP routers.

ip dvmrp flash-interval *seconds*

Syntax Definitions

seconds Specifies the interval value, in seconds (5–86400).

Defaults

parameter	default
<i>seconds</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Because routing table change messages are sent between the transmission of complete routing tables, the flash update interval value must be lower than the route report interval.

Examples

```
-> ip dvmrp flash-interval 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip dvmrp](#) Displays global DVMRP parameters.

MIB Objects

```
alaDvmrpGlobalConfig  
  alaDvmrpFlashUpdateInterval
```

ip dvmrp graft-timeout

Configures the graft message retransmission value. The graft message retransmission value is the duration of time that the routing switch will wait before retransmitting a graft message if it has not received an acknowledgement from its neighbor.

ip dvmrp graft-timeout *seconds*

Syntax Definitions

seconds Specifies the graft message retransmission value, in seconds (5–86400).

Defaults

parameter	default
<i>seconds</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp graft-timeout 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip dvmrp](#) Displays global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig
alaDvmrpGraftRetransmission

ip dvmrp interface

Enables or disables the DVMRP protocol on a specified interface.

ip dvmrp interface {*interface_name*}

no ip dvmrp interface {*interface_name*}

Syntax Definitions

interface_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to delete an interface.

Examples

```
-> ip dvmrp interface vlan-10  
-> no ip dvmrp interface vlan-10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp admin-state	Globally enables or disables the DVMRP protocol on the switch.
ip dvmrp interface metric	Configures the distance metric for an interface, which is used to calculate distance vectors.
show ip dvmrp interface	Displays information for all multicast-capable interfaces.

MIB Objects

dvmrpInterfaceTable
 dvmrpInterfaceLocalAddress
 dvmrpInterfaceStatus

ip dvmrp interface metric

Configures the distance metric for an interface, which is used to calculate distance vectors. DVMRP uses the distance metric value to determine the most cost-effective way to pass data through the network.

ip dvmrp interface *{interface_name}* **metric** *value*

Syntax Definitions

interface_name The name of the interface.
value Specifies the metric value (1–31).

Defaults

parameter	default
<i>value</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

DVMRP uses the distance metric value to determine the most cost-effective way to pass data through the network. The higher the distance metric value, the higher the cost.

Examples

```
-> ip dvmrp interface vlan-2 metric 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip dvmrp interface](#) Enables or disables the DVMRP protocol on a specified interface.
[show ip dvmrp interface](#) Displays the DVMRP interface table.

MIB Objects

dvmrpInterfaceTable
 dvmrpInterfaceLocalAddress
 dvmrpInterfaceMetric

ip dvmrp neighbor-interval

Configures the neighbor probe interval time. The neighbor probe interval time specifies how often probes are transmitted on DVMRP-enabled interfaces.

ip dvmrp neighbor-interval *seconds*

Syntax Definitions

seconds Specifies the probe interval time, in seconds (5–30).

Defaults

parameter	default
<i>seconds</i>	10

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp neighbor-interval 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- [ip dvmrp neighbor-timeout](#) Configures the neighbor timeout.
- [show ip dvmrp neighbor](#) Displays the DVMRP neighbor table.
- [show ip dvmrp](#) Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig
alaDvmrpNeighborProbeInterval

ip dvmrp neighbor-timeout

Configures the neighbor timeout. This value specifies how long the switch will wait for activity from a neighboring DVMRP router before assuming that the inactive router is down.

ip dvmrp neighbor-timeout *seconds*

Syntax Definitions

seconds Specifies the neighbor timeout, in seconds (5–86400).

Defaults

parameter	default
<i>seconds</i>	35

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp neighbor-timeout 35
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- [ip dvmrp neighbor-interval](#) Configures the neighbor probe interval time.
- [show ip dvmrp neighbor](#) Displays the DVMRP neighbor table.
- [show ip dvmrp](#) Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig
alaDvmrpNeighborTimeout

ip dvmrp prune-lifetime

Indicates the length of time a prune will be in effect—i.e., its *lifetime*. When the prune lifetime expires, the interface is joined back onto the multicast delivery tree. If unwanted multicast datagrams continue to arrive, the prune mechanism will be re-initiated and the cycle will continue.

ip dvmrp prune-lifetime *seconds*

Syntax Definitions

seconds Specifies the prune lifetime, in seconds (180–86400).

Defaults

parameter	default
<i>seconds</i>	7200

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp prune-lifetime 7200
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp prune-timeout	Configures the prune packet retransmission value.
show ip dvmrp prune	Displays DVMRP prune entries, including the router's upstream prune state.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig
alaDvmrpPruneLifetime

ip dvmrp prune-timeout

Configures the prune packet retransmission value. This value is the duration of time that the routing switch will wait if it continues to receive unwanted multicast traffic before retransmitting a prune message.

ip dvmrp prune-timeout *seconds*

Syntax Definitions

seconds Specifies retransmission time, in seconds (30–86400).

Defaults

parameter	default
<i>seconds</i>	30

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp prune-timeout 30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp prune-lifetime	Indicates the length of time a prune will be in effect.
show ip dvmrp prune	Displays DVMRP prune entries, including the router's upstream prune state.
show ip dvmrp	Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig
alaDvmrpPruneRetransmission

ip dvmrp report-interval

Configures the route report interval. This value defines how often the switch will send its complete routing table to neighboring routers running DVMRP.

ip dvmrp report-interval *seconds*

Syntax Definitions

seconds Specifies the report interval, in seconds (10–2000).

Defaults

parameter	default
<i>seconds</i>	60

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp report-interval 60
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- [show ip dvmrp route](#) Displays the DVMRP routes that are being advertised to other routers.
- [show ip dvmrp](#) Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig
 alaDvmrpRouteReportInterval

ip dvmrp route-holddown

Configures the time during which DVMRP routes are kept in a hold down state. A holddown state refers to the time that a route to an inactive network continues to be advertised.

ip dvmrp route-holddown *seconds*

Syntax Definitions

seconds Specifies the holddown time, in seconds (1–86400).

Defaults

parameter	default
<i>seconds</i>	120

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp route-holddown 120
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp route-timeout	Configures the route expiration timeout value.
show ip dvmrp	Displays the global DVMRP parameters.
show ip dvmrp route	Displays the DVMRP routes that are being advertised to other routers.

MIB Objects

alaDvmrpGlobalConfig
alaDvmrpRouteHoldDown

ip dvmrp route-timeout

Configures the route expiration timeout value. The route expiration timeout value specifies how long the switch will wait before aging out a route. When the route expiration timeout expires, the route is advertised as being in holddown until either its activity resumes or it is deleted from the route table.

ip dvmrp route-timeout *seconds*

Syntax Definitions

seconds Specifies the timeout value, in seconds (20–4000).

Defaults

parameter	default
<i>seconds</i>	140

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip dvmrp route-timeout 140
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip dvmrp route-holddown](#) Configures the time during which DVMRP routes are kept in a hold down state.

[show ip dvmrp](#) Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig
alaDvmrpRouteExpirationTimeout

ip dvmrp subord-default

Changes the initial default assumption on a neighbor's subordinate or non-subordinate status. When the status value is true, DVMRP neighbors are assumed to be subordinate and traffic is automatically forwarded to the neighbor upon initial discovery. When the value is false, traffic is not forwarded to the neighbor until route reports have been exchanged and the neighbor has explicitly expressed dependency.

ip dvmrp subord-default {true | false}

Syntax Definitions

true	DVMRP neighbors are assumed subordinate; traffic is automatically forwarded to the neighbor on initial discovery.
false	DVMRP neighbors are <i>not</i> assumed to be subordinate; traffic is not forwarded until route reports have been exchanged and the neighbor has explicitly expressed dependency.

Defaults

parameter	default
true false	true

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- However, if neighbors in the DVMRP domain have difficulty handling large initial bursts of traffic, it is recommended that the neighbor's default status as a subordinate be changed to false.
- To view the current subordinate neighbor status, use the **show ip dvmrp** command. For more information, refer to [page 25-19](#).

Examples

```
-> ip dvmrp subord-default false
```

Release History

Release 7.1.1; command was introduced.

Related Commands**show ip dvmrp**

Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig

 alaDvmrpInitNbrASSubord

ip interface tunnel

Configures the end points for the GRE and IPIP tunnels.

ip interface *name* **tunnel** [**source** *ip_address*] [**destination** *ip_address*] [**protocol** {**ipip** | **gre**}]

no ip dvmrp interface *name*

Syntax Definitions

<i>name</i>	Text string up to 20 characters. Use quotes around string if description contains multiple words with spaces between them (e.g. "Alcatel-Lucent Marketing"). Note that this value is case sensitive.
source <i>ip_address</i>	Source IP address of the tunnel.
destination <i>ip_address</i>	Destination IP address of the tunnel.
ipip	Specifies the tunneling protocol as IPIP.
gre	Specifies the tunneling protocol as GRE.

Defaults

parameter	default
ipip gre	ipip

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You can configure an interface as either a vlan or tunnel interface.
- The maximum number of GRE tunnel interfaces that can be configured on a switch is 8.
- The maximum number of IPIP tunnel interfaces that can be configured on a switch is 127.
- Use the **no** form of this command to remove an IP interface.

Examples

```
-> ip interface "tnl-1" tunnel source 23.23.23.1 destination 155.2.2.2 protocol gre
-> ip interface "tnl-1" tunnel source 23.23.23.1 destination 155.2.2.2 protocol
ipip
```

Release History

Release 7.1.1; command introduced

Related Commands

show ip dvmrp interface

Displays information for all multicast-capable interfaces or for a specified interface. This command also provides options to display only DVMRP-enabled or DVMRP-disabled interfaces.

MIB Objects

```
alaIpInterfaceTable  
  alaIpInterfaceName  
  alaIpInterfaceTunnelSrc  
  alaIpInterfaceTunnelDst  
  alaIpInterfaceDeviceType
```

show ip dvmrp

Displays the global DVMRP parameters.

show ip dvmrp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip dvmrp
```

```
DVMRP Admin Status = enabled,  
Flash Interval      = 5,  
Graft Timeout      = 5,  
Neighbor Interval  = 10,  
Neighbor Timeout   = 35,  
Prune Lifetime     = 7200,  
Prune Timeout      = 30,  
Report Interval    = 60,  
Route Holddown     = 120,  
Route Timeout      = 140,  
Subord Default     = true,
```

```
Number of Routes          = 2,  
Number of Reachable Routes = 2
```

output definitions

DVMRP Admin Status

The current global (i.e., switch-wide) status of DVMRP, which can be **enabled** or **disabled**. To change the current DVMRP global status, refer to the [ip dvmrp admin-state command on page 25-3](#).

Flash Interval

The current minimum flash update interval value, in seconds. The flash interval defines how often routing table change messages are sent to neighboring DVMRP routers. Because routing table change messages are sent between the transmission of complete routing tables, the flash update interval must be shorter than the route report interval. The default value is 5.

output definitions (continued)

Graft Timeout	The graft message retransmission value, in seconds. The graft message retransmission value defines the duration of time that the routing switch will wait before retransmitting a graft message if it has not received an acknowledgement from its neighbor. Values may range from 5–86400. The default value is 5.
Neighbor Interval	The current neighbor probe interval time, in seconds. The neighbor probe interval time specifies how often probes are transmitted to interfaces with attached DVMRP neighbors. Values may range from 5–30. The default value is 10.
Neighbor Timeout	The current neighbor timeout value, in seconds. This value specifies how long the routing switch will wait for activity from a neighboring DVMRP router before assuming the inactive router is down. Values may range from 5–86400. The default value is 35.
Prune Lifetime	The length of time, in seconds, a prune will be in effect. When the prune lifetime expires, the interface is joined back onto the multicast delivery tree. If unwanted multicast datagrams continue to arrive, the prune mechanism will be re-initiated and the cycle will continue. Values may range from 180–86400. The default value is 7200.
Prune Timeout	The current prune packet retransmission value, in seconds. This value indicates the duration of time that the routing switch will wait if it continues to receive unwanted multicast traffic before retransmitting a prune message. Values range from 30–86400. The default value is 30.
Report Interval	The current route report interval, in seconds. The route report interval defines how often routers will send their complete routing tables to neighboring routers running DVMRP. Values may range from 10–2000. The default value is 60.
Route Holddown	The current holddown time, in seconds. This value indicates the time during which DVMRP routes are kept in a holddown state. A holddown state refers to the time that a route to an inactive network continues to be advertised. Values may range from 1–120. The default value is 120.
Route Timeout	The current route expiration timeout value, in seconds. The route expiration timeout value specifies how long the routing switch will wait before aging out a route. Values may range from 20–4000. The default value is 140.
Subord Default	Displays the initial default assumption on a neighbor's subordinate or non-subordinate status. When the status value is true, DVMRP neighbors are assumed to be subordinate and traffic is automatically forwarded to the neighbor upon initial discovery. When the value is false, traffic is not forwarded to the neighbor until route reports have been exchanged and the neighbor has explicitly expressed dependency. To change the current subordinate neighbor status, refer to the ip dvmrp subord-default command on page 25-15 . Options include true and false. The default value is true.

output definitions (continued)

Number of Routes	The number of entries in the routing table. This number can be used to monitor the routing table size and detect illegal advertisements of unicast routes.
Number of Reachable Routes	The total number of reachable routes. The number of entries in the routing table with non-infinite metrics. This number can be used to detect network partitions by observing the ratio of reachable routes to total routes. Routes with unreachable metrics, routes in a holddown state, and routes that have aged out are not considered reachable.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp admin-state	Globally enables or disables DVMRP protocol on the switch.
ip dvmrp flash-interval	Configures the minimum flash update interval value.
ip dvmrp graft-timeout	Configures the graft message retransmission value.
ip dvmrp neighbor-timeout	Configures the neighbor timeout.
ip dvmrp prune-lifetime	Indicates the length of time a prune will be in effect.
ip dvmrp prune-timeout	Configures the prune packet retransmission value.
ip dvmrp report-interval	Configures the route report interval.
ip dvmrp route-holddown	Configures the time during which DVMRP routes are kept in a hold down state.
ip dvmrp route-timeout	Configures the route expiration timeout value.
ip dvmrp subord-default	Configures the neighbor probe interval time.

MIB Objects

```

alaDvmrpConfigMIBGroup
  alaDvmrpAdminStatus
  alaDvmrpRouteReportInterval
  alaDvmrpFlashUpdateInterval
  alaDvmrpNeighborTimeout
  alaDvmrpRouteExpirationTimeout
  alaDvmrpRouteHoldDown
  alaDvmrpNeighborProbeInterval
  alaDvmrpPruneLifetime
  alaDvmrpPruneRetransmission
  alaDvmrpGraftRetransmission
  alaDvmrpInitNbrAsSubord

dvmrpGeneralGroup
  dvmrpNumRoutes
  dvmrpReachableRoutes

```

show ip dvmrp interface

Displays information for all multicast-capable interfaces *or* for a specified interface. This command also provides options to display only DVMRP-enabled or DVMRP-disabled interfaces.

show ip dvmrp interface [*ip_address* | *interface_name* | **enabled** | **disabled**]

Syntax Definitions

<i>ip_address</i>	Specifies a particular interface IP address.
<i>interface_name</i>	The name of the interface.
enabled	Displays a list of all interfaces (i.e., VLAN router ports) on which DVMRP is currently <i>enabled</i> .
disabled	Displays a list of all interfaces (i.e., VLAN router ports) on which DVMRP is currently <i>disabled</i> .

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If no optional syntax is specified in the command line, the entire interface table is displayed.
- For an interface to show as *enabled* in the **show ip dvmrp interface** or **show ip dvmrp interface enabled** output, the interface must be both administratively *and* operationally enabled. Although the interface does not have to be passing traffic, at least one VLAN router port must be operational on the corresponding DVMRP-enabled VLAN.
- To view the Generation ID being used on a particular interface, you must include the interface IP address in the command line.

Examples

```
-> show ip dvmrp interface
Interface Name      Vlan  Metric  Admin-Status  Oper-Status
-----+-----+-----+-----+-----
vlan-1              1      1      Disabled      Disabled
vlan-2              2      1      Enabled       Enabled

-> show ip dvmrp interface enabled
Interface Name      Vlan  Metric  Admin-Status  Oper-Status
-----+-----+-----+-----+-----
vlan-2              2      1      Enabled       Enabled
```

output definitions

Interface Name	The name of the interface.
Vlan	The associated VLAN ID.
Tunnel	Indicates whether there is a DVMRP tunnel currently configured on the interface.
Metric	The current metric value. A metric is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.
Admin-Status	The current administrative status of the corresponding interface. Options include Enabled or Disabled . An interface can be configured for DVMRP without being operational. To change the DVMRP Admin-status for an individual interface, refer to the ip dvmrp interface command on page 25-6 .
Oper-Status	The current operational status of the corresponding multicast-capable interface. Options include Enabled or Disabled . For an interface to be DVMRP-operational, the global DVMRP status must be enabled and the individual interface must be DVMRP-enabled. To change the global DVMRP status, refer to the ip dvmrp admin-state command on page 25-3 .

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip dvmrp interface](#) Enables or disables the DVMRP protocol on a specified interface.

MIB Objects

```
dvmrpInterfaceGroup
  dvmrpInterfaceLocalAddress
  dvmrpInterfaceMetric
  dvmrpInterfaceStatus
```

show ip dvmrp neighbor

Displays the DVMRP neighbor table. The DVMRP neighbor table displays either all neighboring DVMRP routers, or a specified neighboring DVMRP router.

show ip dvmrp neighbor [*ip_address*]

Syntax Definitions

ip_address Specifies a particular IP address for a neighboring DVMRP router.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If a neighbor IP address is not specified, the entire DVMRP Neighbor Table is displayed.

Examples

```
-> show ip dvmrp neighbor
```

```
Neighbor Address  Intf Name      Uptime        Expires        GenID        Vers  State
-----+-----+-----+-----+-----+-----+-----
143.209.92.214   vlan-2         00h:09m:12s  00h:00m:06s  546947509   3.255  active
```

output definitions

Neighbor Address	The 32-bit IP address of the DVMRP neighbor's router interface.
Intf Name	The interface name of the neighbor's router.
Uptime	The amount of time the neighbor has been running, displayed in hours, minutes, and seconds.
Expires	The amount of time remaining before the neighbor expires, displayed in hours, minutes, and seconds.
GenID	The generation ID for the DVMRP neighbor. This value is used by neighboring routers to detect whether the DVMRP routing table should be resent.
Version	The DVMRP version number for the neighbor.
State	The current state of the DVMRP neighbor. Options include active and down .

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip dvmrp neighbor-interval** Configures the neighbor probe interval time.
ip dvmrp neighbor-timeout Configures the neighbor timeout.

MIB Objects

```
dvmrpNeighborTable  
  dvmrpNeighborAddress  
  dvmrpNeighborIfIndex  
  dvmrpNeighborUpTime  
  dvmrpNeighborExpiryTime  
  dvmrpNeighborGenerationId  
  dvmrpNeighborMajorVersion  
  dvmrpNeighborMinorVersion  
  dvmrpNeighborState
```

show ip dvmrp nexthop

Displays DVMRP next hop entries. This command is used to show the list of next hops on outgoing interfaces to which IP multicast datagrams from particular sources are routed.

show ip dvmrp nexthop [*ip_address ip_mask*]

Syntax Definitions

<i>ip_address</i>	Specifies a source IP address for which DVMRP next hop entries will be displayed.
<i>ip_mask</i>	Specifies a source IP mask for which DVMRP next hop entries will be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If an IP address and IP mask are not specified, the entire DVMRP Next Hop table is displayed.

Examples

```
-> show ip dvmrp nexthop 172.22.2.115 255.255.255.0
```

Src Address/Mask	Interface Name	Vlan	Hop Type
172.22.2.115/24	vlan-2	2	branch

output definitions

Src Address/Mask	The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
Interface Name	The name of the interface.
Vlan	The associated VLAN ID.
Hop Type	The hop type of the associated entry. Options include leaf or branch . If the next hop VLAN has a DVMRP neighbor attached to it, the hop type will be displayed as branch .

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

dvmrpRouteNextHopTable

dvmrpRouteNextHopSource

dvmrpRouteNextHopSourceMask

dvmrpRouteNextHopIfIndex

 dvmrpRouteNextHopType

show ip dvmrp prune

Displays DVMRP prune entries that have been sent upstream.

show ip dvmrp prune [*group_address source_address source_mask*]

Syntax Definitions

<i>group_address</i>	Specifies a pruned group address.
<i>source_address</i>	Specifies a source IP address.
<i>source_mask</i>	Specifies a source IP mask.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If a group address, source address, and source mask are not specified, the entire Prune table is displayed.

Examples

```
-> show ip dvmrp prune
```

Group Address	Source Address/Mask	Expires
-----+-----+-----		
224.0.0.4	143.209.92.14/24	00h:00m:30s

output definitions

Group Address	The 32-bit multicast group address.
Source Address/Mask	The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
Expires	The amount of time remaining before the current prune state expires, displayed in hours, minutes, and seconds.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip dvmrp prune-lifetime](#)

Indicates the length of time a prune will be in effect.

[ip dvmrp prune-timeout](#)

Configures the prune packet retransmission value.

MIB Objects

dvmrpPruneTable

 dvmrpPruneGroup

 dvmrpPruneSource

 dvmrpPruneSourceMask

 dvmrpPruneExpiryTime

show ip dvmrp route

Displays the DVMRP routes that are being advertised to other routers.

show ip dvmrp route [*ip_address ip_mask*]

Syntax Definitions

ip_address The 32-bit source IP address representing route(s).

ip_mask A 32-bit number that determines the subnet mask for the IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If a source IP address and IP mask are not specified, the entire DVMRP route table is displayed.

Examples

```
-> show ip dvmrp route
Legends:  Flags:  L = Local, R = Remote, F = Flash, H = Holddown, I = Invalid
          Address/Mask      Gateway      Metric      Age          Expires      Flags
-----+-----+-----+-----+-----+-----
          11.0.0.0/8        55.0.0.5    2           00h:13m:14s  02m:07s     R
          22.0.0.0/8        44.0.0.4    2           00h:33m:14s  02m:15s     R
          44.0.0.0/8        -           1           05h:24m:59s  -           L
          55.0.0.0/8        -           1           05h:24m:59s  -           L
          66.0.0.0/8        44.0.0.4    2           00h:03m:11s  02m:15s     R
```

output definitions

Address/Mask	The 32-bit IP address for the router interface, along with the corresponding subnet mask. The interface's subnet mask is shown using the CIDR prefix length: 255.0.0.0 equals /8; 255.255.0.0 equals /16; 255.255.255.0 equals /24, etc.
Gateway	The corresponding 32-bit gateway address. Because it is not applicable, no gateway address is displayed for local routes.
Metric	The current metric value. A metric is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.
Age	The current age of the DVMRP route, displayed in hours, minutes, and seconds.

output definitions (continued)

Expires	The expiration time for the corresponding route. Because it is not applicable, no expiration time is displayed for local routes.
Flags	The flag type of a particular DVMRP route. Options include L (Local), R (Remote), F (Flash), H (Holddown), and I (Invalid).

Release History

Release 7.1.1; command was introduced.

Related Commands

ip dvmrp report-interval	Configures the route report interval.
ip dvmrp route-holddown	Configures the time during which DVMRP routes are kept in a hold down state.
ip dvmrp route-timeout	Configures the route expiration timeout value.

MIB Objects

```
dvmrpRouteTable
  dvmrpRouteSource
  dvmrpRouteSourceMask
  dvmrpRouteMetric
  dvmrpRouteExpiryTime
  dvmrpRouteUpTime
```

show ip dvmrp tunnel

Displays DVMRP tunnel entries.

show ip dvmrp tunnel [*local_address remote_address*]

Syntax Definitions

local_address

The IP address of a particular local router interface. The local router interface IP address is an identifier for the local end of the DVMRP tunnel.

remote_mask

The IP address of a particular remote router interface. The remote router interface IP address is an identifier for the remote end of the DVMRP tunnel.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If optional local and remote IP address information is not specified, entire DVMRP Tunnels table is displayed.
- The local IP address of the tunnel must match the IP address of an existing DVMRP-enabled IP interface.

Examples

-> show ip dvmrp tunnel

Interface Name	Local Address	Remote Address	TTL	Status
vlan-2	143.209.92.203	12.0.0.1	255	Enabled

output definitions

Interface Name	The interface name.
Local Address	The 32-bit local IP address for the DVMRP tunnel.
Remote Address	The 32-bit remote IP address for the DVMRP tunnel.
TTL	The current Time to Live (TTL) value. A value of 0 indicates that the value is copied from the payload's header. Values may range from 0–255.
Status	The corresponding interface status. Options include Enabled or Disabled . If the interface specified by the local address has been configured and is operationally enabled, the status is Enabled . If the interface is down, the value displayed is Disabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip interface tunnel](#)

Adds or deletes a DVMRP tunnel.

[show ip dvmrp](#)

Configures the TTL value for the tunnel defined for the specified local address and remote address.

MIB Objects

tunnelIfTable

- tunnelIfLocalAddress
- tunnelIfRemoteAddress
- tunnelIfHopLimit

dvmrpInterfaceGroup

- dvmrpInterfaceStatus

26 PIM Commands

Protocol-Independent Multicast (PIM) is an IP multicast routing protocol that uses routing information provided by unicast routing protocols, such as RIP and OSPF. Note that PIM is not dependent on any particular unicast routing protocol. Sparse mode PIM (PIM-SM) contrasts with flood-and-prune dense mode multicast protocols, such as DVMRP and PIM Dense Mode (PIM-DM), in that multicast forwarding in PIM-SM is initiated only through specific requests.

Downstream routers must explicitly join PIM-SM distribution trees to receive multicast streams on behalf of directly connected receivers or other downstream PIM-SM routers. This paradigm of receiver-initiated forwarding makes PIM ideal for network environments where receiver groups are thinly populated and bandwidth conservation is a concern, such as in wide area networks (WANs). PIM-DM uses RPF (Reverse Path Forwarding) to prevent looping of multicast datagrams while flooding. If some areas of the network do not have group members, PIM-DM will prune the forwarding branch by instantiating the prune state.

PIM-DM differs from PIM-SM in two essential ways:

- There are no periodic joins transmitted, only explicitly triggered prunes and grafts.
- There is no Rendezvous Point (RP). This is particularly important in networks that cannot tolerate a single point of failure.

Alcatel-Lucent implementation of PIM can also be configured in an IPv6 environment.

MIB information for the PIM commands is as follows:

Filename: AlcatelIND1Pim_mib.htm
Module: ALCATEL-IND1-PIM-MIB

Filename: AlcatelIND1PimBsrDraft_mib.htm
Module: ALCATEL-IND1-PIM-BSR-MIB

Filename: AlcatelIND1PimStdDraft_mib.htm
Module: ALCATEL-IND1-PIM-STD-MIB

A summary of the available commands is listed here:

ip load pim	show ip pim static-rp
ip pim sparse admin-state	show ip pim cbsr
ip pim dense admin-state	show ip pim bsr
ip pim ssm group	show ip pim notifications
ip pim dense group	show ip pim groute
ip pim cbsr	show ip pim sgroute
ip pim static-rp	ipv6 pim sparse admin-state
ip pim candidate-rp	ipv6 pim dense admin-state
ip pim rp-threshold	ipv6 pim ssm group
ip pim keepalive-period	ipv6 pim dense group
ip pim max-rps	ipv6 pim cbsr
ip pim probe-time	ipv6 pim static-rp
ip pim register checksum	ipv6 pim candidate-rp
ip pim register-suppress-timeout	ipv6 pim rp-switchover
ip pim spt admin-state	ipv6 pim spt admin-state
ip pim state-refresh-interval	ipv6 pim interface
ip pim state-refresh-limit	show ipv6 pim sparse
ip pim state-refresh-ttl	show ipv6 pim dense
ip pim interface	show ipv6 pim ssm group
ip pim neighbor-loss-notification-period	show ipv6 pim dense group
ip pim invalid-register-notification-period	show ipv6 pim interface
ip pim invalid-joinprune-notification-period	show ipv6 pim neighbor
ip pim rp-mapping-notification-period	show ipv6 pim static-rp
ip pim interface-election-notification-period	show ipv6 pim group-map
show ip pim sparse	show ipv6 pim candidate-rp
show ip pim dense	show ipv6 pim cbsr
show ip pim ssm group	show ipv6 pim bsr
show ip pim dense group	show ipv6 pim groute
show ip pim neighbor	show ipv6 pim sgroute
show ip pim candidate-rp	
show ip pim group-map	
show ip pim interface	

ip load pim

Dynamically loads PIM to memory.

ip load pim

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command must be executed before PIM can run on the switch.
- This command is supported in both IPv4 and IPv6 PIM.
- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

Examples

```
-> ip load pim
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim sparse admin-state	Globally enables or disables the PIM-SM protocol on the switch.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
ip pim dense admin-state	Globally enables or disables PIM-DM protocol on the switch.
show ip pim dense	Displays the status of the various global parameters for the PIM Dense mode.
ipv6 pim sparse admin-state	Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.
ipv6 pim dense admin-state	Enables or disables the IPv6 PIM-DM (dense mode) globally for IPv6.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

alaDrcTmConfig
alaDrcTmIPpimStatus

ip pim sparse admin-state

Globally enables or disables PIM-SM protocol on the switch.

ip pim sparse admin-state {enable | disable}

Syntax Definitions

enable	Globally enables PIM-SM on the switch.
disable	Globally disables PIM-SM on the switch.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command must be set to **enable** before PIM-SM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to [page 26-3](#) for more information.
- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

Examples

```
-> ip pim sparse admin-state enable
-> ip pim sparse admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
  alaPimsmAdminStatus
```

ip pim dense admin-state

Globally enables or disables PIM-DM protocol on the switch.

`ip pim dense admin-state {enable | disable}`

Syntax Definitions

enable	Globally enables PIM-DM on the switch.
disable	Globally disables PIM-DM on the switch.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command must be set to **enable** before PIM-DM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to [page 26-3](#) for more information.
- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

Examples

```
-> ip pim dense admin-state enable
-> ip pim dense admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
  alaPimdmAdminStatus
```

ip pim ssm group

Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).

```
ip pim ssm group group_address/prefix_length [[no] override] [priority priority]
```

```
no ip pim ssm group group_address/prefix_length
```

Syntax Definitions

<i>group_address</i>	Specifies a 32-bit group address.
<i>/prefix_length</i>	Specifies the prefix length of the multicast group.
override	Specifies the static SSM mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
<i>priority</i>	Specifies the preference value to be used for this static SSM mode configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a SSM mode group mapping.
- The PIM Source-Specific Multicast (SSM) mode for the default SSM address range (232.0.0.0 through 232.255.255.255) reserved by the Internet Assigned Numbers Authority is not enabled automatically and needs to be configured manually to support SSM.
- You can also map additional multicast address ranges for the SSM group using this command. However, the multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the **override** option.
- Note that once the priority option has been defined, a value of 65535 can be used to un-set the priority

Examples

```
-> ip pim ssm group 224.0.0.0/4 priority 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- show ip pim sparse** Displays the status of the various global parameters for the PIM sparse mode.
- show ip pim ssm group** Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.
- show ip pim group-map** Displays the PIM group mapping table.

MIB Objects

```
alaPimStaticRPTable  
  alaPimStaticRPGrpAddress  
  alaPimStaticRPGrpPrefixLength  
  alaPimStaticRPOverrideDynamic  
  alaPimStaticRPPrecedence  
  alaPimStaticRPRowStatus
```

ip pim dense group

Statically maps the specified IP multicast group(s) to the PIM Dense mode (DM).

ip pim dense group *group_address/prefix_length* [[**no**] **override**] [**priority** *priority*]

no ip pim dense group *group_address/prefix_length*

Syntax Definitions

<i>group_address</i>	Specifies a 32-bit group address.
<i>/prefix_length</i>	Specifies the prefix length of the multicast group.
override	Specifies this static Dense mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
<i>priority</i>	Specifies the preference value to be used for this static configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a dense mode group mapping.
- This command specifies the mode as Dense (PIM-DM) for the specified multicast group address.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to un-set the priority.

Examples

```
-> ip pim dense group 224.0.0.0/4 priority 50
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ip pim dense group	Displays the static configuration of multicast group mappings for PIM-Dense Mode (DM).
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimStaticRPTable  
  alaPimStaticRPGrpAddress  
  alaPimStaticRPGrpPrefixLength  
  alaPimStaticRPOverrideDynamic  
  alaPimStaticRPPrecedence  
  alaPimStaticRPRowStatus
```

ip pim cbsr

Configures the local router as the Candidate-BSR for the PIM domain.

ip pim cbsr *ip_address* [**priority** *priority*] [**mask-length** *bits*]

no ip pim cbsr *ip_address*

Syntax Definitions

<i>ip_address</i>	Specifies the 32-bit address that the local router uses to advertise itself as a Candidate-BSR.
<i>priority</i>	Specifies the priority value of the local router as a Candidate-BSR. The higher the value, the higher the priority. Values may range from 0 to 255.
<i>bits</i>	Specifies a 32-bit mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group). Values may range from 1 to 32.

Defaults

parameter	default
<i>priority</i>	64
<i>bits</i>	30

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the local routers candidature as the BSR.
- This command is supported only in the sparse mode.
- The information configured using this command is used in the Bootstrap messages.
- Candidate-BSRs also avoid a single point of failure in a PIM domain.

Examples

```
-> ip pim cbsr 50.1.1.1 priority 100 mask-length 4
```

Release History

Release 7.1.1; command was introduced.

Related Commands

`show ip pim cbsr`

Displays the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBSrCandidateBSRTable  
  alaPimBsrCandidateBSRAddress  
  alaPimBsrCandidateBSRPriority  
  alaPimBsrCandidateBSRHashMaskLength  
  alaPimBsrCandidateBSRRowStatus
```

ip pim static-rp

Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

ip pim static-rp *group_address/prefix_length rp_address* [[**no**] **override**] [**priority** *priority*]

no ip pim static-rp *group_address/prefix_length rp_address*

Syntax Definitions

<i>group_address</i>	Specifies a 32-bit group address.
<i>/prefix_length</i>	Specifies the prefix length of the multicast group.
<i>rp_address</i>	Specifies a 32-bit Rendezvous Point (RP) address.
override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
<i>priority</i>	Specifies the preference value to be used for the static RP configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a static RP configuration.
- Specifying the priority value obsoletes the **override** option.
- The PIM Source-Specific Multicast (SSM) mode for the default SSM address range (232.0.0.0 through 232.255.255.255) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM. You can also map additional multicast address ranges for the SSM group. However, the multicast groups in the reserved address range can be mapped only to the SSM mode.
- This command is supported only in the sparse mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Note that once the priority option has been defined, a value of 65535 can be used to un-set the priority
- To view current static RP configuration settings, use the [show ip pim static-rp](#) command.

Examples

```
-> ip pim static-rp 224.0.0.0/4 10.1.1.1 priority 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|------------------------------|---|
| show ip pim sparse | Displays the status of the various global parameters for the PIM sparse mode. |
| show ip pim static-rp | Displays the PIM static RP table for ASM mode, which includes group address/prefix length, the static Rendezvous Point (RP) address, and the current status of static RP configuration (i.e., enabled or disabled). |
| show ip pim group-map | Displays the PIM group mapping table. |

MIB Objects

```
alaPimStaticRPTable  
  alaPimStaticRPGrpAddress  
  alaPimStaticRPGrpPrefixLength  
  alaPimStaticRPPAddress  
  alaPimStaticRPOverrideDynamic  
  alaPimStaticRPPrecedence  
  alaPimStaticRPRowStatus
```

ip pim candidate-rp

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IP multicast group(s).

ip pim candidate-rp *rp_address* *group-address/prefix_length* [**priority** *priority*] [**interval** *seconds*]

no ip pim candidate-rp *rp_address* *group-address/prefix_length*

Syntax Definitions

<i>rp_address</i>	Specifies a 32-bit address that will be advertised as a Candidate-RP.
<i>group_address</i>	Specifies a 32-bit group address for which the local router will advertise itself as a Candidate-RP.
<i>/prefix_length</i>	Specifies the prefix length of the multicast group.
<i>priority</i>	Specifies the priority value of the Candidate-RP. Values may range from 0 to 192. The lower the value, the higher the priority.
<i>seconds</i>	Specifies the interval at which the C-RP advertisements are sent to the bootstrap router, in seconds. Values may range from 1 to 300.

Defaults

parameter	default
<i>priority</i>	192
<i>seconds</i>	60

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a C-RP for a particular multicast group.
- The specified *rp_address* must belong to a PIM enabled interface.
- Only one RP address is supported per switch. If multiple candidate-RP entries are defined, they must specify the same *rp-address*.
- The priority and the interval values are used by the switch. If they are modified for one entry, the switch will modify these for all the candidate-rp entries.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim candidate-rp 50.1.1.1 224.0.0.0/4 priority 100 interval 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim candidate-rp Displays the IP multicast groups for which the local router will advertise itself as a Candidate-RP.

MIB Objects

```
alaPimBsrCandidateRPTable  
  alaPimBsrCandidateRPAddress  
  alaPimBsrCandidateRPGroupAddress  
  alaPimBsrCandidateRPGroupPrefixLength  
  alaPimBsrCandidateRPPriority  
  alaPimBsrCandidateRPAdvInterval  
  alaPimBsrCandidateRPRowStatus
```

ip pim rp-threshold

Specifies the data rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing a source-specific (S, G) Join message toward the source.

ip pim rp-threshold *bps*

Syntax Definitions

bps The data rate value, in bits per second, at which the RP will attempt to switch to native forwarding (0–2147483647).

Defaults

parameter	default
<i>bps</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is supported only in the sparse mode.
- To disable the RP threshold feature, specify a bits per second value of 0. When the RP threshold is disabled, the RP will never initiate an (S, G) Join message toward the source; the packets will be register-encapsulated to the RP. It will issue a (S, G) Join message upon receiving the first data packet, if its bits per second value is 1.
- To view the current RP threshold, use the [show ip pim sparse](#) command.

Examples

```
-> ip pim rp-threshold 131072
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip pim sparse](#) Displays the global parameters for PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig  
  alaPimsmRPThreshold
```

ip pim keepalive-period

Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.

ip pim keepalive-period *seconds*

Syntax Definitions

seconds Specifies the timeout value, in seconds (0-65535).

Defaults

parameter	default
<i>seconds</i>	210

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This timer is called the Keepalive Period in the PIM-SM specification and the Source Lifetime in the PIM-DM specification.
- This command includes support for both IPv4 PIM and IPv6 PIM.

Examples

```
-> ip pim keepalive-period 500
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

alaPim
alaPimKeepalivePeriod

ip pim max-rps

Configures the maximum number of C-RP routers allowed in the PIM-SM domain.

ip pim max-rps *number*

Syntax Definitions

number The maximum number of C-RP routers allowed in the PIM-SM domain (1–100).

Defaults

parameter	default
<i>number</i>	32

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is supported only in the sparse mode.
- This command is used with both IPv4 and IPv6 PIM-SM. The PIM-SM must be disabled before changing **max-rps** value.
- PIM-SM must be globally disabled before changing the maximum number of C-RP routers. To globally disable PIM-SM, refer to the [ip pim sparse admin-state](#) command on page 26-5.

Examples

```
-> ip pim max-rps 32
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim sparse admin-state	Globally enables or disables the PIM-SM protocol on the switch.
ipv6 pim sparse admin-state	Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.
show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

alaPimsmGlobalConfig
alaPimsmMaxRPs

ip pim probe-time

Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.

ip pim probe-time *seconds*

Syntax Definitions

seconds The probe time, in seconds (1–300).

Defaults

parameter	default
<i>seconds</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used with both IPv4 and IPv6 PIM-SM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim probe-time 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

alaPismGlobalConfig
 alaPismProbeTime

ip pim register checksum

Configures the application of the checksum function on sent and received register messages in the domain.

ip pim register checksum {header | full}

Syntax Definitions

header	Specifies that the checksum for registers is done only on the PIM header.
full	Specifies that the checksum is done over the entire PIM register message.

Defaults

parameter	default
header full	header

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **full** option may be required for compatibility with older implementations of PIM-SM v2.
- This parameter setting must be consistent across the PIM domain.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim register checksum header
-> ip pim register checksum full
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip pim sparse](#) Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
  alaPimsmOldRegisterMessageSupport
```

ip pim register-suppress-timeout

Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.

ip pim register-suppress-timeout *seconds*

Syntax Definitions

seconds The timeout value, in seconds (0–65535).

Defaults

parameter	default
<i>seconds</i>	60

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is supported in both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim register-suppress-timeout 10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip pim sparse	Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

alaPim
alaPimRegisterSuppressionTime

ip pim spt admin-state

Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first data packet is received.

ip pim spt admin-state {enable | disable}

Syntax Definitions

enable	Enables last hop DR switching to the SPT.
disable	Disables last hop DR switching to the SPT.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is supported only in the sparse mode.
- As mentioned above, if SPT status is enabled, last hop DR switching to the SPT begins once the first data packet is received.
- To view whether SPT status is currently enabled (default) or disabled, use the [show ip pim sparse](#) command.

Examples

```
-> ip pim spt admin-state enable
-> ip pim spt admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip pim sparse](#) Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
  alaPimsmAdminSPTConfig
```

ip pim state-refresh-interval

Sets the interval between successive State Refresh messages originated by a router.

ip pim state-refresh-interval *seconds*

Syntax Definitions

seconds The interval between successive State Refresh messages, in seconds. Values may range from 0 to 65535.

Defaults

parameter	default
<i>seconds</i>	60

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 PIM-DM and IPv6 PIM-DM.

Examples

```
-> ip pim state-refresh-interval 80
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ipv6 pim interface	Enables IPv6 PIM and configures the statistics.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

alaPim
alaPimRefreshInterval

ip pim state-refresh-limit

Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.

ip pim state-refresh- limit *ticks*

Syntax Definitions

ticks

The limit at which the received State Refresh messages will not be forwarded, if the messages are received at less than the interval. Values may range from 0 to 65535.

Defaults

parameter	default
<i>ticks</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 and IPv6.

Examples

```
-> ip pim state-refresh-limit 2
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim interface	Enables or disables the PIM protocol on a specific interface.
ipv6 pim interface	Enables IPv6 PIM and configures the statistics.
show ip pim dense	Displays the status of the various global parameters for the PIM dense mode.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

alaPimdmGlobalConfig
alaPimdmStateRefreshLimitInterval

ip pim interface

Enables PIM and configures PIM-related statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the interface.

ip pim interface *if_name* [**hello-interval** *seconds*] [**triggered-hello** *seconds*] [**joinprune-interval** *seconds*] [**hello-holdtime** *seconds*] [**joinprune-holdtime** *seconds*] [**prune-delay** *milliseconds*] [**override-interval** *milliseconds*] [**dr-priority** *priority*] [[**no**] **stub**] [**prune-limit-interval** *seconds*] [**graft-retry-interval** *seconds*]

no ip pim interface *if_name*

Syntax Definitions

<i>if_name</i>	The interface name on which PIM is being enabled or disabled.
hello-interval <i>seconds</i>	The frequency at which PIM Hello messages are transmitted on a specified interface, in seconds. Values may range from 0 to 18000.
triggered-hello <i>seconds</i>	Specifies the maximum time, in seconds, before a triggered PIM Hello message is sent on this interface. Values may range from 0 to 60.
joinprune-interval <i>seconds</i>	The frequency at which periodic Join/Prune messages are sent on this interface, in seconds. Values may range from 0 to 18000.
hello-holdtime <i>seconds</i>	Specifies the value set in the Holdtime field of PIM Hello messages sent on this interface, in seconds. Values may range from 0 to 65535.
joinprune-holdtime <i>seconds</i>	Specifies the value inserted into the Holdtime field of the Join/Prune messages sent on this interface, in seconds. Values may range from 0 to 65535.
prune-delay <i>milliseconds</i>	Specifies the value of the expected propagation delay between PIM routers on this network, inserted into the LAN prune-delay option of the Hello messages sent on this interface, in milliseconds. Values may range from 0 to 32767.
override-interval <i>milliseconds</i>	Specifies the value inserted into the Override Interval field of the LAN prune-delay option of the Hello messages sent on this interface, in <i>milliseconds</i> . Values may range from 0 to 65535.
dr-priority <i>priority</i>	Specifies the Designated Router priority inserted into the DR priority option on a specified interface. The DR priority option value can range between 1 to 192. A higher numeric value denotes a higher priority.
prune-limit-interval <i>seconds</i>	Specifies the minimum interval that must elapse between two successive prune messages sent on this interface, in seconds. Values may range from 0 to 65535.
graft-retry-interval <i>seconds</i>	Specifies the minimum interval that must elapse between two successive graft messages sent on this interface, in seconds. Values may range from 0 to 65535.
stub	Specifies the interface not to send any PIM packets through this interface, and to ignore received PIM packets.

Defaults

parameter	default
hello-interval <i>seconds</i>	30
triggered-hello <i>seconds</i>	5
joinprune-interval <i>seconds</i>	60
hello-holdtime <i>seconds</i>	105
joinprune-holdtime <i>seconds</i>	210
prune-delay <i>milliseconds</i>	500
override-interval <i>milliseconds</i>	2500
dr-priority <i>priority</i>	1
prune-limit-interval <i>seconds</i>	60
graft-retry-interval <i>seconds</i>	3
stub	Disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a PIM interface.
- PIM must be enabled globally on the switch before it runs on the interface. To globally enable or disable PIM-SM on the switch, refer to the [ip pim sparse admin-state command on page 26-5](#). To enable or disable PIM-DM on the switch, refer to the [ip pim dense admin-state command on page 26-6](#).
- Specifying zero for the hello-interval represents an infinite time, in which case periodic PIM Hello messages are not sent.
- Specifying zero for the joinprune-interval represents an infinite time, in which case periodic PIM Join/Prune messages are not sent.
- Specifying the value of 65535 for hello-holdtime represents an infinite time. If a PIM router gets Hello packet from a neighbor with its hello-holdtime value as infinite time, then the PIM router will not time out the sender(neighbor). It is recommended that you should use a hello-holdtime interval that is 3.5 times the value of the hello-interval, or 65535 seconds if the hello-interval is set to zero.
- Specifying the value of 65535 for joinprune-holdtime represents an infinite time. The receipt of Join/Prune messages with its joinprune-holdtime value as infinite time, then this specifies an infinite hold-time for the particular join/prune message. It is recommended that you use a joinprune-holdtime interval that is 3.5 times the value of the Join/Prune interval defined for the interface, or 65535 seconds if the joinprune-interval is set to zero.
- The interface configured as a **stub** will not send any PIM packets through that interface, and any received PIM packets are also ignored. By default, a PIM interface is not set to be a stub one.
- The **graft-retry-interval** and **prune-limit-interval** options can be used only with the PIM-DM mode.

Examples

```
-> ip pim interface vlan-2 hello-interval 100 triggered-hello 10 joinprune-interval 100 hello-holdtime 350 joinprune-holdtime 400
-> no ip pim interface vlan-2
```

Release History

Release 7.1.1; command was introduced.

Related Command

[show ip pim interface](#)

Displays detailed PIM settings for a specific interface. In general, it displays PIM settings for all the interfaces if no argument is specified.

MIB Objects

```
alaPimInterfaceTable
  alaPimInterfaceIfIndex
  alaPimInterfaceStatus
  alaPimInterfaceHelloInterval
  alaPimInterfaceTrigHelloInterval
  alaPimInterfaceJoinPruneInterval
  alaPimInterfaceHelloHoldtime
  alaPimInterfaceJoinPruneHoldtime
  alaPimInterfacePropagationDelay
  alaPimInterfaceOverrideInterval
  alaPimInerfaceDRPriority
  alaPimInterfaceStubInterface
  alaPimInterfacePruneLimitInterval
  alaPimInterfaceGraftRetryInterval
```

ip pim neighbor-loss-notification-period

Specifies the minimum time that must elapse between PIM neighbor loss notifications originated by the router.

ip pim neighbor-loss-notification-period *seconds*

Syntax Definitions

seconds Specifies the time value that must elapse between neighbor loss notifications, in seconds (0–65535).

Defaults

parameter	default
<i>seconds</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The maximum value of 65535 represents an infinite time. The PIM neighbor loss notifications are never sent in case of infinite time.
- This command is used with both IPv4 and IPv6 PIM.

Examples

```
-> ip pim neighbor-loss-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip pim notifications](#) Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

alaPim
alaPimNeighborLossNotificationPeriod

ip pim invalid-register-notification-period

Specifies the minimum time that must elapse between the PIM invalid register notifications originated by the router.

ip pim invalid-register-notification-period *seconds*

Syntax Definitions

seconds Specifies the minimum time value that must elapse between invalid register notifications, in seconds (10–65535).

Defaults

parameter	default
<i>seconds</i>	65535

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The default value of 65535 represents an infinite time. The PIM invalid register notifications are never sent in case of infinite time.
- The non-zero minimum allowed value provides resilience against the propagation of denial-of-service attacks from the data and control planes to the network management plane.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim invalid-register-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip pim notifications](#) Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

alaPim
alaPimInvalidRegisterNotificationPeriod

ip pim invalid-joinprune-notification-period

Specifies the minimum time that must elapse between the PIM invalid joinprune notifications originated by the router.

ip pim invalid-joinprune-notification-period *seconds*

Syntax Definitions

seconds Specifies the minimum time value that must elapse between invalid joinprune notifications, in seconds (10–65535).

Defaults

parameter	default
<i>seconds</i>	65535

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The default value of 65535 represents an infinite time. The PIM invalid joinprune notifications are never sent in case of infinite time.
- The non-zero minimum allowed value provides resilience against the propagation of denial-of-service attacks from the control plane to the network management plane.
- This value is used with both IPv4 and IPv6 PIM.

Examples

```
-> ip pim invalid-joinprune-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip pim notifications](#) Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

alaPim
alaPimInvalidJoinPruneNotificationPeriod

ip pim rp-mapping-notification-period

Specifies the minimum time that must elapse between the PIM RP mapping notifications originated by the router.

ip pim rp-mapping-notification-period *seconds*

Syntax Definitions

seconds Specifies the minimum time value that must elapse between RP mapping notifications, in seconds (0–65535).

Defaults

parameter	default
<i>seconds</i>	65535

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The default value of 65535 represents an infinite time. The RP mapping notifications are never sent in case of infinite time.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim rp-mapping-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip pim notifications](#) Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

alaPim
alaPimRPMappingNotificationPeriod

ip pim interface-election-notification-period

Specifies the minimum time that must elapse between the PIM interface election notifications originated by the router.

ip pim interface-election-notification-period *seconds*

Syntax Definitions

seconds Specifies the minimum time value that must elapse between interface election notifications, in seconds (0–65535).

Defaults

parameter	default
<i>seconds</i>	65535

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The default value of 65535 represents an infinite time. The interface election notifications are never sent in case of infinite time.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ip pim interface-election-notification-period 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip pim notifications](#) Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

alaPim
alaPimInterfaceElectionNotificationPeriod

show ip pim sparse

Displays the status of the various global parameters for the PIM sparse mode.

show ip pim sparse

Syntax Definitions

N/A.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip pim sparse
Status                = enabled,
Keepalive Period      = 210,
Max RPs                = 32,
Probe Time            = 5,
Register Checksum     = header,
Register Suppress Timeout = 60,
RP Threshold          = 1,
SPT Status            = enabled,
```

output definitions

Status	The current global (i.e., switch-wide) status of PIM-SM. Options include enabled and disabled .
Keepalive Period	The duration of the Keepalive timer. The default value is 210.
Max RPs	The maximum number of Rendezvous Points (RPs) allowed in the PIM-SM domain (1–100). The default value is 32.
Probe Time	The amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP. Values may range from 1 to 300. The default value is 5.
Register Checksum	The current application of the checksum function on register messages in the domain. Options include header and full . The default setting is header .
Register Suppress Timeout	The amount of time, in seconds, the Designated Router (DR) will stop sending registers to the Rendezvous Point (RP) once a Register-Stop is received (1–300). The default value is 60.
RP Threshold	Displays the current RP data rate threshold. This value indicates the rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing an (S, G) Join message toward the source. Values may range from 0 to 2147483647. The default value is 1. A value of 0 indicates that the feature is currently disabled.
SPT Status	The current status of last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). Options include enabled and disabled . The default setting is enabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim sparse admin-state	Globally enables or disables PIM-SM protocol on the switch.
ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip pim keepalive-period	Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
ip pim max-rps	Configures the maximum number of C-RP routers allowed in the PIM-SM domain.
ip pim probe-time	Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.
ip pim register checksum	Configures the application of the checksum function on sent and received register messages in the domain.
ip pim register-suppress-timeout	Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.
ip pim rp-threshold	Specifies the data rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing a source-specific (S, G) Join message toward the source.
ip pim spt admin-state	Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first data packet is received.

MIB Objects

```
alaPimsmGlobalConfig
  alaPimsmAdminStatus
  alaPimKeepalivePeriod
  alaPimsmMaxRPS
  alaPimsmProbeTime
  alaPimsmOldRegisterMessageSupport
  alaPimRegisterSuppressionTime
  alaPimsmRPThreshold
  alaPimsmAdminSPTConfig
```

show ip pim dense

Displays the status of the various global parameters for the PIM dense mode.

```
show ip pim dense
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip pim dense
Status                = enabled,
Source Lifetime       = 210,
State Refresh Interval = 60,
State Refresh Limit Interval = 0,
State Refresh TTL     = 16
```

output definitions

Status	The current global (i.e., switch-wide) status of PIM-DM. Options include enabled and disabled .
Source Lifetime	The duration of the Keepalive or Source Lifetime timer. The default value is 210.
State Refresh Interval	The time-interval, in seconds, between successive State Refresh messages originated by the router. The default value is 60.
State Refresh Limit Interval	Displays the limit at which a router will not forward the State Refresh messages, if they are received at less than the interval.
State Refresh TTL	Displays the TTL to be used in the router's originated State Refresh messages. The default value is 16.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim dense admin-state	Globally enables or disables PIM-DM protocol on the switch.
ip pim interface	Enables or disables the PIM protocol on a specific interface.
ip pim state-refresh-interval	Sets the interval between successive State Refresh messages originated by a router.
ip pim state-refresh-limit	Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.
ip pim state-refresh-ttl	Sets the Time to Live to be used in a router's originated State Refresh messages if the data packet's Time to Live is not recorded.
ip pim keepalive-period	Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.

MIB Objects

```

alaPimdmGlobalConfig
  alaPimdmAdminStatus
  alaPimKeepalivePeriod
  alaPimRefreshInterval
  alaPimdmStateRefreshLimitInterval
  alaPimdmStateRefreshTimeToLive

```

show ip pim ssm group

Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.

show ip pim ssm group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- This command is supported only in the sparse mode.

Examples

```
-> show ip pim ssm group
Group Address/Pref Length  Mode  Override  Precedence  Status
-----+-----+-----+-----+-----
224.0.0.0/4                ssm   false    none        enabled
```

output definitions

Group Address/Pref Length	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
Mode	The PIM mode to be used for groups in this prefix. The possible values include asm, ssm, or dm.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include enabled and disabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim ssm group	Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).
show ip pim group-map	Displays the PIM group mapping table.

MIB Objects

```
alaPimStaticRPTable  
  alaPimStaticRPGrpAddress  
  alaPimStaticRPGrpPrefixLength  
  alaPimStaticRPPimMode  
  alaPimStaticRPOverrideDynamic  
  alaPimStaticRPPrecedence  
  alaPimStaticRPRowStatus
```

show ip pim dense group

Displays the static configuration of multicast group mappings for PIM-Dense Mode (DM).

show ip pim dense group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- This command is supported only on PIM dense mode.

Examples

```
-> show ip pim dense group
```

```
Group Address/Pref Length  Mode  Override  Precedence  Status
-----+-----+-----+-----+-----
224.0.0.0/4                dm    false    none        enabled
```

output definitions

Group Address/Pref Length	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
Mode	The PIM mode to be used for groups in this prefix. The possible values include asm, ssm, or dm.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include enabled and disabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim dense group Creates and manages the static configuration of dense mode (DM) group mappings.

show ip pim group-map Displays the PIM group mapping table.

MIB Objects

alaPimStaticRPTable

 alaPimStaticRPGrpAddress
 alaPimStaticRPGrpPrefixLength
 alaPimStaticRPRowStatus
 alaPimStaticRPOverrideDynamic
 alaPimStaticRPPrecedence
 alaPimStaticRPPimMode

show ip pim neighbor

Displays a list of active PIM neighbors.

show ip pim neighbor [*ip_address*]

Syntax Definitions

ip_address The 32-bit IP address for the PIM neighbor.

Defaults

If a neighbor's IP address is not specified, the entire PIM neighbor table is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

To view more detailed information about a particular neighbor, specify the neighbor's IP address in the command line. Additional information will be displayed, which includes LAN Prune Delay, Override Interval, TBit field, State Refresh capable, and Designated Router option status.

Examples

```
-> show ip pim neighbor
Neighbor Address      Interface Name      Uptime      Expires      DR Priority
-----+-----+-----+-----+-----
212.61.20.250        vlan-2             01h:07m:07s 00h:01m:38s 100
212.61.60.200        vlan-6             01h:07m:07s 00h:01m:38s 100
214.28.4.254         vlan-26            01h:07m:07s 00h:01m:38s 100
```

If a specific neighbor IP address is specified in the command line, *detailed information for the corresponding neighbor only* displays:

```
-> show ip pim neighbor 212.61.30.7
Neighbor IP Address   = 212.61.30.7,
Interface Name       = vlan-30,
Uptime               = 00h:04m:14s,
Expires              = 00h:01m:31s,
Lan Prune Delay Present = true,
Propagation Delay    = 500,
Override Interval    = 2500,
TBit field           = false,
Gen ID Present       = true,
Gen ID Value         = 0x79ca868e,
BiDir Capable       = false,
DR Priority Present   = true,
DR Priority           = 1,
State Refresh Capable = true
```

output definitions

Neighbor (IP) Address	The 32-bit IP address of the active PIM neighbor.
Interface Name	The name of the interface used to reach this PIM neighbor.
Uptime	The amount of time since this PIM neighbor last became a neighbor of the local router, displayed in hours, minutes, and seconds.
Expiry time	The minimum amount of time remaining before the PIM neighbor will be aged out, displayed in hours, minutes, and seconds.
Lan Prune Delay Present	Evaluates to TRUE if this neighbor is using the Lan Prune Delay option.
Propagation Delay	The expected propagation delay between PIM routers on this network.
DR Priority Present	Evaluates to TRUE if the neighbor is using the DR Priority option.
DR Priority	The value of the Designated Router Priority from the last PIM Hello message received from this neighbor. This object is always zero if the DR Priority Present value is FALSE.
TBit field	The value of the Tbit field of the LAN prune delay option received from this neighbor. The Tbit specifies the ability of the neighbor to disable Join suppression.
Generation ID Present	Evaluates to TRUE if this neighbor is using the Generation ID option.
Generation ID Value	The value of the Generation ID from the last PIM Hello message received from the neighbor.
BiDir Capable	Evaluates to TRUE if this neighbor is using the Bidirectional-PIM Capable option.
State Refresh Capable	Displays whether the neighbor is capable of receiving State Refresh messages. Options include true or false .
Override Interval	The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```

alaPimNeighborTable
  alaPimNeighborAddress
  alaPimNeighborIfIndex
  alaPimNeighborUpTime
  alaPimNeighborExpiryTime
  alaPimNeighborLanPruneDelayPresent
  alaPimNeighborPropagationDelay
  alaPimNeighborTBit

```

```
alaPimNeighborGenerationIDPresent  
alaPimNeighborGenerationIDValue  
alaPimNeighborBidirCapable  
alaPimNeighborDRPriorityPresent  
alaPimNeighborDRPriority  
alaPimNeighborOverrideInterval  
alaPimNeighborSRCapable
```

show ip pim candidate-rp

Displays the IP multicast groups for which the local router advertises itself as a Candidate-RP.

show ip pim candidate-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip pim candidate-rp
RP Address          Group Address      Priority  Interval  Status
-----+-----+-----+-----+-----
172.21.63.11       224.0.0.0/4       192      60        enabled
```

output definitions

RP Address	A 32-bit IP address that is advertised as the Candidate-Rendezvous Point (RP).
Group Address	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/). This is the group for which the local router advertises itself as a C-RP.
Priority	The C-RP router's priority. The lower the value, the higher the priority.
Interval	The time interval at which the C-RP advertisements are sent to the BSR.
Status	The current status of this entry. The status is shown as enabled only if the PIM-SM is globally enabled and the PIM interface is enabled.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip pim candidate-rp](#)

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IP multicast group(s).

MIB Objects

```
alaPimBsrCandidateRPTable  
  alaPimBsrCandidateRPAddress  
  alaPimBsrCandidateRPGroupAddress  
  alaBsrCandidateRPGroupPrefixLength  
  alaPimBsrCandidateRPPriority  
  alaPimBsrCandidateRPInterval  
  alaPimBsrCandidateRPStatus
```

show ip pim group-map

Displays the PIM group mapping table.

show ip pim group-map [**bsr** | **static-rp** | **ssm** | **dense**]

Syntax Definitions

N/A

Defaults

If the keywords **bsr**, **static-rp**, **ssm**, or **dense** are included in the command line, then only the entries that were created by the specified origin are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined through the **ip pim static-rp** command. As long as the RP addresses defined in the static RP set are reachable, they will be added to the group mapping table.
- If the IP multicast groups are mapped to the mode SSM or DM, then the entries created by local SSM address range configuration using the **ip pim ssm group** command and local Dense Mode address range configuration using the **ip pim dense group** command are displayed.
- If the bootstrap mechanism is being used, this information is obtained from received Candidate-RP advertisements (when the local router is the BSR; when the local router is not the BSR, this information is obtained from received bootstrap messages).

Examples

```
-> show ip pim group-map
```

Origin	Group Address/Pref Length	RP Address	Mode	Precedence
BSR	224.0.0.0/4	172.21.63.11	asm	192
BSR	224.0.0.0/4	214.0.0.7	asm	192
Static	232.0.0.0/8		ssm	

```
-> show ip pim group-map bsr
```

Origin	Group Address/Pref Length	RP Address	Mode	Precedence
BSR	224.0.0.0/4	172.21.63.11	asm	192
BSR	224.0.0.0/4	214.0.0.7	asm	192

```
-> show ip pim group-map static
```

Origin	Group Address/Pref Length	RP Address	Mode	Precedence
Static	232.0.0.0/8		ssm	

output definitions

Origin	The mechanism by which the PIM mode and RP for the group were learned. The possible values include 'static RP' for local static RP configuration, 'static SSM' for both SSM group configuration and Dense Mode Group configuration, and 'BSR' for the PIM Bootstrap Router mechanism.
Group Address/Prefix Length	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
RP Address	The IP address of the Rendezvous Point to be used for groups within the group prefix. There is no RP address if the PIM mode is either SSM or DM.
Mode	The PIM mode to be used for groups in this prefix.
Mapping Precedence	The precedence value of a particular row, which determines which row applies to a given group address. Numerically higher values for this object indicate lower precedences, with the value zero denoting the highest precedence.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim ssm group	Creates and manages the static configuration of a Source Specific Multicast mode group mappings.
ip pim dense group	Creates and manages the static configuration of dense mode (DM) group mappings.
ip pim static-rp	Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

MIB Objects

```
alaPimGroupMappingTable
  alaPimGroupMappingOrigin
  alaPimGroupMappingGrpAddress
  alaPimGroupMappingPrecedence
  alaPimGroupMappingRPAddress
  alaPimGroupMappingPimMode
  alaPimGroupMappingGrpPrefixLength
```

show ip pim interface

Displays detailed PIM settings for a specific interface. In general, it displays PIM settings for all the interfaces if no argument is specified.

show ip pim interface [*if_name*]

Syntax Definitions

if_name The interface name.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

To view more detailed information about a particular interface, specify the interface name in the command line. Additional information includes Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

Examples

```
-> show ip pim interface
Total 1 Interfaces
```

Interface Name	IP Address	Designated Router	Hello Interval	J/P Interval	Oper Status
tesvl	50.1.1.1	50.1.1.1	100	10	disabled

```
-> show ip pim interface tesvl
Interface Name           = tesvl,
IP Address               = 50.1.1.1,
Designated Router       = 50.1.1.1,
Hello Interval          = 30,
Triggered Hello Interval = 5,
Hello HoldTime          = 105,
Join/Prune Interval     = 60,
Join/Prune HoldTime     = 210,
Propagation (Prune) Delay = 500,
Override Interval       = 2500,
Generation ID           = 0x46e68b13,
DR Priority              = 1,
DR Priority Enabled     = true,
Lan Delay Enabled       = true,
Effective Propagation Delay = 500,
Effective Override Interval = 2500,
Suppression Enabled     = true,
```

```

Stub Interface           = false,
Prune Limit Interval    = 60,
Graft Retry Interval    = 3,
State Refresh Enabled   = true,
Operational Status      = disabled

```

output definitions

Interface Name	The name of the interface on which PIM is enabled.
IP address	Specifies the IP address of the specified interface.
Designated Router	The 32-bit IP address for the Designated Router (DR). The DR acts on behalf of any directly-connected hosts with respect to the PIM-SM protocol. Only one router in the LAN will act as the DR.
Hello Interval	The frequency at which PIM Hello messages are transmitted on a specified interface. Values may range from 1 to 18000. The default value is 30.
Join/Prune Interval	The Join/Prune interval for the associated interface. The Join/Prune interval is the interval at which periodic PIM-SM Join/Prune messages are sent. Values may range from 1 to 18000.
Triggered Hello Interval	The current Triggered Hello Interval. This value indicates the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface. Values may range from 1 to 60. The default value is 5.
Hello Holdtime	The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 105.
Join/Prune Holdtime	The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 210.
Propagation Delay	The expected propagation delay between PIM routers on this network.
Override Interval	The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.
Generation ID Option	The value of the Generation ID this router inserted in the last PIM Hello message it sent on this interface.
DR Priority	Displays the Designated Router priority for each interface. This value is used in determining the Designated Router on an interface. Values may range from 1 to 192. A higher numeric value denotes a higher priority. Note that priority-based election is used only if all routers on the interface are using the DR priority option. The default value is 1.
Lan Delay Enabled	Options include true and false . The value will be true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting will be false.
Effective Propagation Delay	The Effective Propagation Delay on this interface.

output definitions (continued)

Effective Override Interval	The Effective Override Interval on this interface.
Suppression Enabled	Specifies whether the Join suppression is enabled on this interface.
DR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the DR Priority option.
Stub Interface	Specifies whether this interface is a 'stub interface'. If this is TRUE, then no PIM packets are sent out on this interface, and any received PIM packets are ignored.
Prune Limit Interval	The minimum interval that must transpire between two successive Prunes sent by a router. This is used only with PIM-DM.
Graft Retry Interval	Displays the time-interval a router waits for a Graft acknowledgment before resending a Graft on the interface. This is used only with PIM-DM. Values may range from 1 to 65535. The default value is 3.
SR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the State Refresh option. This is used only by PIM-DM.
Operational Status	The current operational status of the corresponding interface. Options include enabled and disabled . This value indicates whether the IP interface is operationally up. For example, if PIM is enabled on the interface, but the IP interface is currently down, this field will display as disabled. The default setting is disabled . To globally enable or disable PIM on the switch, refer to the ip pim sparse admin-state command on page 26-5 and ip pim dense admin-state command on page 26-6 .

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip pim interface](#) Enables or disables the PIM protocol on a specific interface.

MIB Objects

```
alaPimInterfaceTable
  alaPimInterfaceIfIndex
  alaPimInterfaceDR
  alaPimInterfaceHelloInterval
  alaPimInterfaceJoinPruneInterval
  alaPimInterfaceStatus
  alaPimInterfaceAddress
  alaPimInterfaceTrigHelloInterval
  alaPimInterfaceHelloHoldtime
  alaPimInterfaceJoinPruneHoldtime
  alaPimInterfacePropagationDelay
  alaPimInterfaceOverrideInterval
  alaPimInterfaceGenerationIDValue
  alaPimInterfaceDRPriority
  alaPimInterfaceLanDelayEnabled
  alaPimInterfaceEffectPropagDelay
  alaPimInterfaceEffectOverrideIvl
```

```
alaPimInterfaceSuppressionEnabled  
alaPimInterfaceDRPriorityEnabled  
alaPimInterfaceStubInterface  
AlaPimInterfacePruneLimitInterval  
alaPimInterfaceGraftRetryInterval  
alaPimInterfaceSRPriorityEnabled
```

show ip pim static-rp

Displays the PIM Static RP table for the ASM mode, which includes group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the Static RP configuration (i.e., enabled or disabled).

```
show ip pim static-rp
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range

Examples

```
-> show ip pim static-rp
Group Address/Pref Length  RP Address      Mode  Override Precedence Status
-----+-----+-----+-----+-----+-----
224.0.0.0/4                172.21.63.11  asm   false    none     enabled
```

output definitions

Group Address/Pref Length	The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/). To change the current multicast group address and mask, refer to the ip pim static-rp command on page 26-13 .
RP Address	A 32-bit IP address of the Rendezvous Point (RP). To change the current RP address, refer to the ip pim static-rp command on page 26-13 .
Mode	The PIM mode to be used for groups in this prefix. The possible values include asm, ssm, or dm.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	Specifies the precedence value to be used for this static RP configuration.
Status	Displays whether static RP configuration is currently enabled or disabled. Options include enabled and disabled . To change the current status, refer to the ip pim static-rp command on page 26-13 .

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip pim static-rp](#)

Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

MIB Objects

```
alaPimStaticRPTable
  alaPimStaticRPGrpAddress
  alaPimStaticRPGrpPrefixLength
  alaPimStaticRPAddress
  alaPimStaticRPPimMode
  alaPimStaticRPOverrideDynamic
  alaPimStaticRPPrecedence
  alaPimStaticRPRowStatus
```

show ip pim cbsr

Displays the Candidate-BSR information that is used in the Bootstrap messages.

show ip pim cbsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip pim cbsr
CBSR Address           = 214.0.0.7,
Status                 = enabled,
CBSR Priority           = 0,
Hash Mask Length       = 30,
Elected BSR           = False,
Timer                  = 00h:00m:00s
```

output definitions

CBSR Address	The 32-bit address that the local router uses to advertise itself as a Candidate-BSR.
Status	The current status of this entry. The status is shown as enabled only if the PIM-SM is globally enabled and the PIM interface is enabled.
CBSR Priority	The value for the local router as a Candidate-BSR. The higher the value, the higher the priority.
Hash Mask Length	The 32-bit mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group.
Elected BSR	Specifies whether the local router is the elected BSR.
Timer	The time value that is remaining before the local router originates the next bootstrap message. This value is zero if this router is not the elected BSR.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip pim cbsr](#)

Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBSrCandidateBSRTable  
  alaPimBsrCandidateBSRAddress  
  alaPimBsrCandidateBSRPriority  
  alaPimBsrCandidateBSRHashMaskLength  
  alaPimBsrCandidateBSRElectedBSR  
  alaPimBsrCandidateBSRBootstrapTimer  
  alaPimBsrCandidateBSRStatus
```

show ip pim bsr

Displays information about the elected BSR.

show ip pim bsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip pim bsr
BSR Address           = 214.0.0.7
BSR Priority           = 192,
Hash Mask Length      = 30,
Expiry Time           = 00h:01m:35s
```

output definitions

BSR Address	The 32-bit address of the elected BSR.
BSR Priority	The priority value of the elected BSR. The higher the value, the higher the priority.
Hash Mask Length	The 32-bit mask length that is advertised in the bootstrap messages by the elected BSR (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group).
Expiry Time	The minimum time remaining before the elected BSR will be declared down.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ip pim cbsr](#)

Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBsrElectedBSRTable  
  alaPimBsrElectedBSRAddress  
  alaPimBsrElectedBSRPriority  
  alaPimBsrElectedBSRHashMaskLength  
  alaPimBsrElectedBSRExpiryTime
```

show ip pim notifications

Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

show ip pim notifications

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The outputs from this command includes both IPv4 and IPv6 information.

Examples

```
-> show ip pim notifications
Neighbor Loss Notifications
  Period      = 0
  Count       = 0
Invalid Register Notifications
  Period      = 65535
  Msgs Rcvd   = 0
  Origin      = None
  Group       = None
  RP          = None
Invalid Join Prune Notifications
  Period      = 65535
  Msgs Rcvd   = 0
  Origin      = None
  Group       = None
  RP          = None
RP Mapping Notifications
  Period      = 65535
  Count       = 0
Interface Election Notifications
  Period      = 65535
  Count       = 0
```

output definitions

Neighbor Loss Notification	Period: Minimum time interval that must elapse between the PIM neighbor loss notification originated by the device. Count: The number of neighbor loss events that have occurred. This counter is incremented whenever a neighbor loss notification is generated.
Invalid Register Notification	Period: Minimum time interval that must elapse between the PIM invalid register notifications originated by the device. Msgs Rcvd: The number of invalid PIM register notification messages that have been received by the device. Group: The multicast group address to which the last unexpected Register message received by the device was addressed. RP: The RP address to which the last unexpected Register message received by the device was delivered. Origin: The source address of the last unexpected Register message received by the device.
Invalid Join/Prune Notification	Period: Minimum time that must elapse between PIM invalid join-prune notifications originated by the device. Msgs Rcvd: The number of invalid PIM join/prune messages that have been received by the device. Origin: The source address of the last unexpected join/prune message received by the device. Group: The multicast group address carried in the last unexpected join-prune message received by the device. RP: The RP address carried in the last unexpected join/prune message received by the device.
RP Mapping Notifications	Period: Minimum time that must elapse between PIM RP mapping change notifications originated by the device. Count: The number of changes to active RP mappings on this device.
Interface Election Notifications	Period: Minimum time that must elapse between PIM Interface Election traps originated by the router. Count: The number of times this device has been elected DR on any interface.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip pim neighbor-loss-notification-period

Specifies the minimum time that must elapse between PIM neighbor loss notifications originated by the router.

ip pim invalid-register-notification-period

Specifies the minimum time that must elapse between PIM invalid register notifications originated by the router.

ip pim invalid-joinprune-notification-period

Specifies the minimum time that must elapse between PIM invalid joinprune notifications originated by the router.

ip pim rp-mapping-notification-period

Specifies the minimum time that must elapse between PIM RP mapping notifications originated by this router.

ip pim interface-election-notification-period

Specifies the minimum time that must elapse between the PIM interface election notifications originated by the router.

MIB Objects

alaPim

```
alaPimNeighborLossNotificationPeriod
alaPimNeighborLossCount
alaPimInvalidRegisterNotificationPeriod
alaPimInvalidRegisterMsgsRcvd
alaPimInvalidRegisterGroup
alaPimInvalidRegisterRp
alaPimInvalidJoinPruneNotificationPeriod
alaPimInvalidJoinPruneMsgsRcvd
alaPimInvalidJoinPruneOrigin
alaPimInvalidJoinPruneGroup
alaPimInvalidJoinPruneRP
alaPimRPMappingNotificationPeriod
alaPimRPMappingChangeCount
alaPimInterfaceElectionNotificationPeriod
alaPimInterfaceElectionWinCount
```

show ip pim groute

Displays all (*,G) state that the IPv4 PIM has.

show ip pim groute [*group_address*]

Syntax Definitions

group_address A 32-bit multicast address. If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

Defaults

By default, entire (*,G) routing table is displayed. To view more detailed (*,G) state information about a particular group, specify the group address in the command line.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When the *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.

Examples

```
-> show ip pim groute
```

```
Total 1 (*,G)
```

Group Address	RP Address	RPF Interface	Upstream Neighbor	UpTime
225.0.0.0	212.61.60.8	vlan-30	212.61.30.7	00h:01m:43s
225.0.0.1	212.61.60.8	vlan-30	212.61.30.7	00h:01m:43s

```
-> show ip pim groute 225.0.0.0
```

```
(*,225.0.0.0)
```

```
UpTime           = 00h:01m:49s
RP Address       = 212.61.60.8,
PIM Mode        = ASM,
PIM Mode Origin = BSR,
Upstream Join State = Joined,
Upstream Join Timer = 00h:00m:11s,
Upstream Neighbor = 212.61.30.7,
RPF Interface    = vlan-30,
RPF Next Hop     = 212.61.30.7,
RPF Route Protocol = OSPF,
RPF Route Address = 212.61.60.0/24,
RPF Route Metric Pref = 110,
RPF Route Metric = 2,
Interface Specific State:
  vlan-4
    UpTime           = 00h:01m:49s,
```



```

Local Membership          = True,
Join/Prune State         = No Info,
Prune Pending Timer      = 00h:00m:00s,
Join Expiry Timer        = 00h:00m:00s,
Assert State             = No Info,
Assert Timer             = 00h:00m:00s,
vlan-5
UpTime                   = 00h:00m:00s,
Local Membership         = False,
Join/Prune State         = No Info,
Prune Pending Timer      = 00h:00m:00s,
Join Expiry Timer        = 00h:00m:00s,
Assert State             = No Info,
Assert Timer             = 00h:00m:00s,
vlan-8
UpTime                   = 00h:00m:00s,
Local Membership         = False,
Join/Prune State         = No Info,
Prune Pending Timer      = 00h:00m:00s,
Join Expiry Timer        = 00h:00m:00s,
Assert State             = No Info,
Assert Timer             = 00h:00m:00s,
vlan-9
UpTime                   = 00h:00m:00s,
Local Membership         = False,
Join/Prune State         = No Info,
Prune Pending Timer      = 00h:00m:00s,
Join Expiry Timer        = 00h:00m:00s,
Assert State             = No Info,
Assert Timer             = 00h:00m:00s,
vlan-30
UpTime                   = 00h:00m:00s,
Local Membership         = False,
Join/Prune State         = No Info,
Prune Pending Timer      = 00h:00m:00s,
Join Expiry Timer        = 00h:00m:00s,
Assert State             = No Info,
Assert Timer             = 00h:00m:00s,

```

output definitions

Group-address	The IPv4 Multicast Group Address.
RP Address	The address of the Rendezvous Point (RP) for the group.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (*,G) join messages to.
UpTime	The time since this entry was created.
Pim Mode Origin	The mechanism by which the PIM mode and RP for the group were learned.
Upstream Join State	Whether the local router should join the RP tree for the group.
Upstream Join Timer	The time remaining before the local router next sends a periodic (*,G) Join message on the RPF IfIndex.
RPF Next Hop	The address of the RPF next hop towards the RP.

output definitions (continued)

RPF Route Protocol	The routing mechanism through which the route used to find the RPF interface towards the RP was learned.
RPF Route Address/Prefix Length	The IPv6 address combined with the prefix length identifies the route used to find the RPF interface towards the RP.
Route Metric Pref	The metric preference of the route used to find the RPF interface towards the RP.
Route Metric	The routing metric of the route used to find the RPF interface towards the RP.
Interface Name	The interface name that corresponds to the ifIndex.
Local Membership	Whether the local router has (*,G) local membership on this interface.
Join Prune State	The state resulting from (*,G) Join/Prune messages received on this interface.
Prune Pending Timer	The time remaining before the local router acts on a (*,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.
Join Expiry Timer	The time remaining before (*,G) Join state for this interface expires.
Assert State	The (*,G) Assert state for this interface. The possible values are No Info, Winner or Loser.
Assert Timer	If Assert State is 'Winner', this is the time remaining before the local router next sends a (*,G) Assert message on this interface. If the Assert State is 'Loser', this is the time remaining before the (*,G) assert state expires.
Assert Winner Address	If the Assert State is 'Loser', this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is 'Loser', this is the metric preference of the route to the RP advertised by the assert winner; otherwise, this is zero.
Assert Winner Metric	If the Assert State is 'Loser', this is the routing metric of the route to the RP advertised by the assert winner; otherwise, this is zero.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaPimStarGTable
  alaPimStarGGrpAddress
  alaPimStarGRPAddress
  alaPimStarGRPFIfIndex
  alaPimStarGUpstreamNeighbor
  alaPimStarGUpTime
  alaPimStarGPimModeOrigin
  alaPimStarGUpstreamJoinState
  alaPimStarGUpstreamJoinTimer
  alaPimStarGRPNextHop
```

```
alaPimStarGRPFRouteProtocol
alaPimStarGRPFRouteAddress
alaPimStarGRPFRoutePrefixLength
alaPimStarGRPFRouteMetricPref
alaPimStarGRPFRouteMetric
alaPimStarGITable
alaPimStarGIIfIndex
alaPimStarGILocalMembership
alaPimStarGIJoinPruneState
alaPimStarGIPrunePendingTimer
alaPimStarGIPrunePendingTimer
alaPimStarGIAssertState
alaPimStarGIAssertTimer
alaPimStarGIAssertWinnerAddress
alaPimStarGIAssertWinnerAddress
alaPimStarGIAssertWinnerMetric
```

show ip pim sgroute

Displays all (S,G) state that the IPv4 PIM has.

show ip pim sgroute [*source_address group_address*]

Syntax Definitions

source_address The 32-bit IP address for a specific multicast source.

group_address A 32-bit multicast address.

Defaults

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the *source_address* and *group_address* associated with that entry.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When the *source_address* and *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

Examples

```
-> show ip pim sgroute
```

```
Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
          L = Local, R = RPT, T = SPT, F = Register,
          P = Pruned, O = Originator
```

```
Total 1 (S,G)
```

Source Address	Group Address	RPF Interface	Upstream Neighbor	UpTime	Flags
172.21.63.2	225.0.0.0	vlan-30	212.61.30.7	00h:02m:09s	ST
172.21.63.2	225.0.0.1	vlan-30	212.61.30.7	00h:02m:09s	ST

```
-> show ip pim sgroute 172.21.63.2 225.0.0.0
(172.21.63.2,225.0.0.0)
```

```
UpTime                    = 00h:02m:16s
PIM Mode                  = ASM,
Upstream Join State      = Joined,
Upstream RPT State       = Not Pruned,
Upstream Join Timer      = 00h:00m:44s,
Upstream Neighbor       = 212.61.30.7,
RPF Interface            = vlan-30,
RPF Next Hop             = 212.61.30.7,
RPF Route Protocol       = OSPF,
RPF Route Address        = 172.21.63.0/24,
RPF Route Metric Pref   = 110,
RPF Route Metric        = 2,
```

```

SPT Bit                = True,
DR Register State      = No Info,
DR Register Stop Timer = 00h:00m:00s,
Interface Specific State:
  vlan-4
    UpTime                = 00h:02m:16s,
    Local Membership       = True,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
  vlan-5
    UpTime                = 00h:00m:00s,
    Local Membership       = False,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
  vlan-8
    UpTime                = 00h:00m:00s,
    Local Membership       = False,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
  vlan-9
    UpTime                = 00h:00m:00s,
    Local Membership       = False,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
  vlan-30
    UpTime                = 00h:00m:00s,
    Local Membership       = False,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,

```

output definitions

Source-address	The IPv4 Source address.
Group-address	The IPv4 Multicast Group Address.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.

output definitions (continued)

Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (S,G) join messages to.
UpTime	The time since this entry was created.
Flags	Flags indicating SPTBit, Prune State, Join State, etc.
Pim Mode	Whether the Group Address is SSM, ASM or DM.
Upstream Join State	Whether the local router should join the SPT for the source and group represented by this entry.
Upstream Join Timer	The time remaining before the local router next sends a periodic (S,G) Join message.
RPF Next Hop	The address of the RPF next hop towards the source.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF Interface towards the source was learned.
RPF Route Address/Prefix Length	The IP address which when combined with the Route Prefix length identifies the route used to find the RPF interface towards the source.
RPF Route Metric Pref	The metric preference of the route used to find the RPF interface towards the source.
RPF Route Metric	The metric preference of the route used to find the RPF interface towards the source.
DR Register State	Whether the local router should encapsulate (S,G) data packets in Register messages and send them to the RP. The possible values include No Info, Join, Join Pending, or Prune.
DR Register Stop Timer	The value of the Register Stop Timer. If the Register State is 'prune', this is the time remaining before the local router sends a Null-Register message to the RP. If the State is 'joinPending', this is the time remaining before the local router resumes encapsulating data packets and sending them to the RP.
Upstream Prune State	Whether the local router has pruned itself from the tree. This is only used by PIM-DM. The possible values include forwarding, Ack Pending, or Pruned.
Upstream Prune Limit Timer	The time remaining before the local router may send a (S,G) prune message on alaPimSGRPFifIndex. This is only used by PIM-DM.
Originator State	Whether this router is an originator for the (S,G) message flow. This is only used by PIM-DM. The possible values include Not Originator or Originator.
Source Active Timer	If this router is the Originator, this is the time remaining before the local router reverts to notOriginator state. Otherwise, this is zero. This is only used by PIM-DM.
State Refresh Timer	If Originator state is 'originator', this is the time remaining before the local router sends a State Refresh Message. Otherwise, this is zero. This is only used by PIM-DM.
Interface Name	The interface name corresponding to the ifIndex that corresponds to this entry.
Uptime	The time since this entry was created.
Local Membership	Whether the local router has (S,G) local membership on this interface.

output definitions (continued)

Join Prune State	The state resulting from (S,G) Join/Prune messages received on this interface. The possible values include No Info, Join, or Prune Pending.
Prune Pending Timer	The time remaining before the local router acts on an (S,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.
Join Expiry Timer	The time remaining before (S,G) Join state for this interface expires.
Assert State	The (S,G) Assert state for this interface. The possible values include No Info, Winner, or Loser.
Assert Timer	If Assert State is Winner, this is the time remaining before the local router sends a (S,G) Assert message on this interface. If the Assert State is Loser, this is the time remaining before the (S,G) Assert state expires.
Assert Winner	If the Assert State is Loser, this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is Loser, this is the metric preference of the route to the source advertised by the assert winner.
Assert Winner Metric Metric	If the Assert State is Loser, this is the routing metric of the route to the source advertised by the assert winner.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```

alaPimSGTable
  alaPimSGSrcAddress
  alaPimSGGrpAddress
  alaPimSGRPFFifIndex
  alaPimSGUpstreamNeighbor
  alaPimSGUpTime
  alaPimSGSPTBit
  alaPimSGUpstreamPruneState
  alaPimSGUpstreamJoinState
  alaPimSGPimMode
  alaPimSGUpstreamJoinState
  alaPimSGUpstreamJoinTimer
  alaPimSGRPFNextHop
  alaPimSGRPFRouteProtocol
  alaPimSGRPFRouteAddress
  alaPimSGRPFRoutePrefixLength
  alaPimSGRPFRouteMetricPref
  alaPimSGRPFRouteMetric
  alaPimSGDRRegisterState
  alaPimSGDRRegisterStopTimer
  alaPimSGUpstreamPruneState
  alaPimSGUpstreamPruneLimitTimer
  alaPimSGOriginatorState

```

```
alaPimSGSourceActiveTimer
alaPimSGStateRefreshTimer
alaPimSGITable
alaPimSGIIfIndex
alaPimSGIUpTime
alaPimSGILocalMembership
alaPimSGIJoinPruneState
alaPimSGIPrunePendingTimer
alaPimSGIJoinExpiryTimer
alaPimSGIAssertState
alaPimSGIAssertTimer
alaPimSGIAssertWinnerAddress
alaPimSGIAssertWinnerMetricPref
alaPimSGIAssertWinnerMetric
```

ipv6 pim sparse admin-state

Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.

ipv6 pim sparse admin-state {enable | disable}

Syntax Definitions

enable	Enables PIM-SM globally for IPv6.
disable	Disables PIM-SM globally for IPv6.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command must be set to **enable** before PIM-SM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to [page 26-3](#) for more information.

Examples

```
-> ipv6 pim sparse admin-state enable
-> ipv6 pim sparse admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ipv6 pim sparse	Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPimsmGlobalConfig
  alaPimsmV6AdminStatus
```

ipv6 pim dense admin-state

Enables or disables the IPv6 PIM-DM (dense mode) globally for IPv6.

ipv6 pim dense admin-state {enable | disable}

Syntax Definitions

enable	Enables PIM-DM globally for IPv6.
disable	Disables PIM-DM globally for IPv6.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command must be set to **enable** before PIM-DM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to [page 26-3](#) for more information.

Examples

```
-> ipv6 pim dense admin-state enable
-> ipv6 pim dense admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim interface	Enables or disables the PIM protocol on a specific interface.
ip load pim	Dynamically loads PIM to memory.
show ipv6 pim dense	Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

```
alaPimdmGlobalConfig
  alaPimdmV6AdminStatus
```

ipv6 pim ssm group

Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

```
ipv6 pim ssm group group_address/prefix_length [[no] override] [priority priority]
```

```
no ipv6 pim ssm group group_address/prefix_length
```

Syntax Definitions

<i>group_address</i>	Specifies the IPv6 multicast group address.
<i>/prefix_length</i>	Specifies the prefix length of the IPv6 multicast group. Values may range from 4 to 128.
override	Specifies the static SSM mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
<i>priority</i>	Specifies the preference value to be used for this static SSM mode configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a Source Specific Multicast mode group mapping.
- The IPv6 PIM Source-Specific Multicast (SSM) mode for the default SSM address range (FF3x::/32) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM.
- You can also map additional IPv6 multicast address ranges for the SSM group using this command. However, the IPv6 multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to un-set the priority.

Examples

```
-> ipv6 pim ssm group ff30::1234:abcd/128 priority 50
-> no ipv6 pim ssm group ff30::1234:abcd/128
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim group-map

Displays the IPv6 PIM group mapping table.

show ipv6 pim ssm group

Displays the static configuration of IPv6 multicast group mappings for PIM-Source Specific Multicast (SSM).

MIB Objects

alaPimStaticRPTable

alaPimStaticRPGrpAddress
alaPimStaticRPGrpPrefixLength
alaPimStaticRPOverrideDynamic
alaPimStaticRPPrecedence
alaPimStaticRPRowStatus

ipv6 pim dense group

Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

```
ipv6 pim dense group group_address/prefix_length [[no] override] [priority priority]
```

```
no ipv6 pim dense group group_address/prefix_length
```

Syntax Definitions

<i>group_address</i>	Specifies the IPv6 multicast group address.
<i>/prefix_length</i>	Specifies the prefix length of the IPv6 multicast group.
override	Specifies the static dense mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
<i>priority</i>	Specifies the preference value to be used for this static configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a static configuration of a dense mode group mapping.
- This command specifies the mode as Dense (PIM-DM) for the specified IPv6 multicast group addresses.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to un-set the priority.

Examples

```
-> ipv6 pim dense group ff0e::1234/128 priority 50  
-> no ipv6 pim dense group ff0e::1234/128
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim group-map

Displays the IPv6 PIM group mapping table.

show ipv6 pim dense group

Displays the static configuration of IPv6 multicast group mappings for PIM Dense Mode (DM).

MIB Objects

alaPimStaticRPTable

alaPimStaticRPGrpAddress

alaPimStaticRPGrpPrefixLength

alaPimStaticRPOverrideDynamic

alaPimStaticRPPrecedence

alaPimStaticRPRowStatus

ipv6 pim cbsr

Configures the local router as the Candidate-BSR for the PIM domain.

ipv6 pim cbsr *ipv6_address* [**priority** *priority*] [**mask-length** *bits*]

no ipv6 pim cbsr *ipv6_address*

Syntax Definitions

<i>ipv6_address</i>	The IPv6 unicast address that the local router will use to advertise itself as a Candidate-BSR. The specified address must be a domain-wide reachable address.
<i>priority</i>	The priority value of the local router as a Candidate-BSR. Values may range from 0 to 255.
<i>bits</i>	The hash mask length that is advertised in the bootstrap messages for IPv6 PIM (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group). Values may range from 1 to 128.

Defaults

parameter	default
<i>priority</i>	64
<i>bits</i>	126

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a Candidate-BSR for a PIM domain.
- This command is supported only in the sparse mode.
- The information configured using this command is used in the Bootstrap messages.
- Candidate-BSRs also avoid a single point of failure in a PIM domain.

Examples

```
-> ipv6 pim cbsr 2000::1 priority 100 mask-length 4
-> no ipv6 pim cbsr 2000::1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

`show ipv6 pim cbsr`

Displays the IPv6 Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBsrCandidateBSRTable  
  alaPimBsrCandidateBSRAddress  
  alaPimBsrCandidateBSRPriority  
  alaPimBsrCandidateBSRHashMaskLength  
  alaPimBsrCandidateBSRRowStatus
```

ipv6 pim static-rp

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

ipv6 pim static-rp *group_address/prefix_length rp_address* [[**no**] **override**] [**priority** *priority*]

no ipv6 pim static-rp *group_address/prefix_length rp_address*

Syntax Definitions

<i>group_address</i>	Specifies the IPv6 multicast group address.
<i>/prefix_length</i>	Specifies the prefix length of the IPv6 multicast group.
<i>rp_address</i>	Specifies the IPv6 unicast address of the Rendezvous Point (RP). This must be a domain-wide reachable address.
override	Specifies the static RP configuration to override the dynamically learned RP information for the specified group(s).
<i>priority</i>	Specifies the preference value to be used for this static RP configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

Defaults

By default, the priority option is not set and the override option is set to false.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a static RP configuration.
- Specifying the priority value obsoletes the **override** option.
- The IPv6 PIM Source-Specific Multicast (SSM) mode for the default SSM address range (FF3x::/32) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM. You can also map additional IPv6 multicast address ranges for the SSM group. However, the IPv6 multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Note that once the priority option has been defined, a value of 65535 can be used to un-set the priority.
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim static-rp ff0e::1234/128 2000::1 priority 10
-> no ipv6 pim static-rp ff0e::1234/128 2000::1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim group-map

Displays the IPv6 PIM group mapping table.

show ipv6 pim static-rp

Displays the IPv6 PIM Static RP table, which includes IPv6 multi-cast group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the Static RP configuration (i.e., enabled or disabled).

MIB Objects

alaPimStaticRPTable

alaPimStaticRPGrpAddress
alaPimStaticRPGrpPrefixLength
alaPimStaticRPRPAddress
alaPimStaticRPOverrideDynamic
alaPimStaticRPPrecedence
alaPimStaticRPRowStatus

ipv6 pim candidate-rp

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IPv6 multicast group(s).

ipv6 pim candidate-rp *rp_address* *group_address/prefix_length* [**priority** *priority*] [**interval** *seconds*]

no ipv6 pim candidate-rp *rp_address* *group_address/prefix_length*

Syntax Definitions

<i>rp_address</i>	Specifies the IPv6 unicast address that will be advertised as a Candidate-RP. This must be a domain-wide reachable address.
<i>group_address</i>	Specifies the IPv6 multicast group address for which the local router will advertise itself as a Candidate-RP.
<i>/prefix_length</i>	Specifies the prefix length of the specified IPv6 multicast group address.
<i>priority</i>	Specifies the priority value of the Candidate-RP. Values may range from 0 to 192. The lower the value, the higher the priority.
<i>seconds</i>	Specifies the interval at which the C-RP advertisements are sent to the bootstrap router, in seconds. Values may range from 1 to 300.

Defaults

parameter	default
<i>priority</i>	192
<i>seconds</i>	60

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a C-RP for a particular multicast group.
- Only one RP address is supported per switch. If multiple candidate-RP entries are defined, they must specify the same *rp-address*.
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim candidate-rp 2000::1 ff0e::1234/128 priority 100 interval 100
-> no ipv6 pim candidate-rp 2000::1 ff0e::1234/128
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim candidate-rp Displays the IPv6 multicast groups for which the local router will advertise itself as a Candidate-RP.

MIB Objects

```
alaPimBsrCandidateRPTable  
  alaPimBsrCandidateRPAddress  
  alaPimBsrCandidateRPGroupAddress  
  alaPimBsrCandidateRPGroupPrefixLength  
  alaPimBsrCandidateRPPriority  
  alaPimBsrCandidateRPAdvInterval  
  alaPimBsrCandidateRPRowStatus
```

ipv6 pim rp-switchover

Enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated packet in the IPv6 PIM domain.

ipv6 pim rp-switchover {enable | disable}

Syntax Definitions

enable	Enables the RP to switch to native forwarding.
disable	Disables the RP from switching to native forwarding.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You cannot specify a pre-configured threshold, such as the RP threshold, as you would do for IPv4 PIM.
- This command is supported only in the sparse mode.

Examples

```
-> ipv6 pim rp-switchover enable
-> ipv6 pim rp-switchover disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim sparse Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

```
alaPismGlobalConfig
  alaPismV6RPSwitchover
```

ipv6 pim spt admin-state

Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT).

ipv6 pim spt admin-state {enable | disable}

Syntax Definitions

enable Enables last hop DR switching to the SPT.

disable Disables last hop DR switching to the SPT.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is supported only in the sparse mode.
- If the SPT status is enabled, last hop DR switching to the SPT begins once the first data packet is received.

Examples

```
-> ipv6 pim spt admin-state enable  
-> ipv6 pim spt admin-state disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 pim sparse](#) Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

alaPimsmGlobalConfig
alaPimsmV6SPTConfig

ipv6 pim interface

Enables IPv6 PIM and configures the statistics such as hello-interval, triggered-hello, hello-holdtime, join-prune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the IPv6 interface.

ipv6 pim interface *if_name* [**hello-interval** *seconds*] [**triggered-hello** *seconds*] [**joinprune-interval** *seconds*] [**hello-holdtime** *seconds*] [**joinprune-holdtime** *seconds*] [**prune-delay** *milliseconds*] [**override-interval** *milliseconds*] [**dr-priority** *priority*] [[**no**] **stub**] [**prune-limit-interval** *seconds*] [**graft-retry-interval** *seconds*]

no ipv6 pim interface *if_name*

Syntax Definitions

<i>if_name</i>	The interface name on which the IPv6 PIM is being enabled or disabled.
hello-interval <i>seconds</i>	The frequency at which IPv6 PIM Hello messages are transmitted on this interface, in seconds. Values may range from 0 to 18000.
triggered-hello <i>seconds</i>	Specifies the maximum time, in seconds, before a triggered IPv6 PIM Hello message is sent on this interface. Values may range from 0 to 60.
joinprune-interval <i>seconds</i>	The frequency at which periodic IPv6 PIM Join/Prune messages are sent on this interface, in seconds. Values may range from 0 to 18000.
hello-holdtime <i>seconds</i>	Specifies the value of the IPv6 PIM hello-holdtime for this interface. This value is set in the Holdtime field of IPv6 PIM Hello messages sent on this interface, in seconds. Values may range from 0 to 65535.
joinprune-holdtime <i>seconds</i>	Specifies the value that is set in the Holdtime field of the IPv6 PIM Joinprune messages sent on this interface, in seconds. Values may range from 0 to 65535.
prune-delay <i>milliseconds</i>	Specifies the value of the expected propagation delay between IPv6 PIM routers on this network, inserted into the LAN prune-delay option of the IPv6 PIM Hello messages sent on this interface, in milliseconds. Values may range from 0 to 32767.
override-interval <i>milliseconds</i>	Specifies the value set in the Override Interval field of the LAN prune-delay option of the IPv6 PIM Hello messages sent on this interface, if the prune-delay status is enabled, in <i>milliseconds</i> . Values may range from 0 to 65535.
dr-priority <i>priority</i>	Specifies the Designated Router priority set in the DR priority option on this interface. The DR priority option value (1–192). A higher numeric value denotes a higher priority.
prune-limit-interval <i>seconds</i>	Specifies the minimum interval that must elapse between two successive IPv6 PIM prune messages sent on this interface, in seconds. Values may range from 0 to 65535.
graft-retry-interval <i>seconds</i>	Specifies the minimum interval that must elapse between two successive IPv6 PIM graft messages sent on this interface, in seconds. Values may range from 0 to 65535.

stub Specifies the interface not to send any IPv6 PIM packets through this interface, and to ignore received IPv6 PIM packets.

Defaults

parameter	default
hello-interval <i>seconds</i>	30
triggered-hello <i>seconds</i>	5
joinprune-interval <i>seconds</i>	60
hello-holdtime <i>seconds</i>	105
joinprune-holdtime <i>seconds</i>	210
prune-delay <i>milliseconds</i>	500
override-interval <i>milliseconds</i>	2500
dr-priority <i>priority</i>	1
prune-limit-interval <i>seconds</i>	60
graft-retry-interval <i>seconds</i>	3
stub	Disabled

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete an IPv6 PIM interface.
- IPv6 PIM must be enabled globally on the switch before IPv6 PIM will begin running on the interface. To globally enable or disable IPv6 PIM-SM on the switch, refer to the [ipv6 pim sparse admin-state command on page 26-75](#). To enable or disable IPv6 PIM-DM on the switch, refer to the [ipv6 pim dense admin-state command on page 26-76](#).
- Specifying zero for IPv6 PIM hello-interval represents an infinite time, in which case the periodic IPv6 PIM hello messages are not sent.
- Specifying zero for IPv6 PIM joinprune-interval represents an infinite time, in which case the periodic IPv6 PIM joinprune messages are not sent.
- Specifying the value of 65535 for IPv6 PIM hello-holdtime represents an infinite time. If an IPv6 PIM router gets IPv6 PIM Hello packet from a neighbor with its hello-holdtime value as infinite time, then the router will not time out the sender(neighbor). It is recommended that you use an IPv6 PIM hello-holdtime interval that is 3.5 times the value of the IPv6 PIM hello-interval, or 65535 seconds if the IPv6 PIM hello-interval is set to zero
- Specifying the value of 65535 for IPv6 PIM joinprune-holdtime represents an infinite time. The receipt of IPv6 Join/Prune messages with its joinprune-holdtime value as infinite time, then this specifies an infinite holdtime for the particular IPv6 join/prune message. It is recommended that you use a join-prune- holdtime interval that is 3.5 times the value of the IPv6 PIM Join/Prune interval defined for the interface, or 65535 seconds if the IPv6 PIM joinprune-interval is set to zero.

- The interface configured as a **stub** will not send any IPv6 PIM packets through that interface, and any received IPv6 PIM packets are also ignored. By default, an IPv6 PIM interface is not set to be a stub one.
- The IPv6 PIM **graft-retry-interval** and **prune-limit-interval** options can be used only with the IPv6 PIM-DM mode.

Examples

```
-> ipv6 pim interface vlan-2 hello-interval 100 triggered-hello 10 joinprune-interval 100 hello-holdtime 350 joinprune-holdtime 400
-> no ipv6 pim interface vlan-2
```

Release History

Release 7.1.1; command was introduced.

Related Command

[show ipv6 pim interface](#) Displays detailed IPv6 PIM settings for a specific interface.

MIB Objects

alaPimInterfaceTable

```
alaPimInterfaceIfIndex
alaPimInterfaceStatus
alaPimInterfaceHelloInterval
alaPimInterfaceTrigHelloInterval
alaPimInterfaceJoinPruneInterval
alaPimInterfaceHelloHoldtime
alaPimInterfaceJoinPruneHoldtime
alaPimInterfacePropagationDelay
alaPimInterfaceOverrideInterval
alaPimInterfaceDRPriority
alaPimInterfaceStubInterface
alaPimInterfacePruneLimitInterval
alaPimInterfaceGraftRetryInterval
```

show ipv6 pim sparse

Displays the status of the various global parameters for the IPv6 PIM sparse mode.

show ipv6 pim sparse

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim sparse
Status                = enabled,
Keepalive Period      = 210,
Max RPs                = 32,
Probe Time            = 5,
Register Suppress Timeout = 60,
RP Switchover         = enabled,
SPT Status            = enabled,
```

output definitions

Status	The current global (i.e., switch-wide) status of the IPv6 PIM sparse mode. Options include enabled and disabled .
Keepalive Period	The duration of the Keepalive timer. The default value is 210.
Max RPs	The maximum number of Rendezvous Points (RPs) allowed in the IPv6 PIM-SM domain (1–100). The default value is 32.
Probe Time	The amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP. Values may range from 1 to 300. The default value is 5.
Register Suppress Timeout	The amount of time, in seconds, the Designated Router (DR) will stop sending registers to the Rendezvous Point (RP) once a Register-Stop is received (1–300). The default value is 60.

output definitions

RP switchover	The current status of the RP Switchover capability. RP switchover enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated data packet. Options include enabled and disabled . The default setting is enabled .
SPT Status	The current status of last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). Options include enabled and disabled . The default setting is enabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim rp-switchover	Enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated packet in the IPv6 PIM domain.
ipv6 pim spt admin-state	Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first multicast data packet is received.
ipv6 pim sparse admin-state	Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.
ipv6 pim interface	Enables IPv6 PIM and configures statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the interface.
ip pim max-rps	Configures the maximum number of C-RP routers allowed in the PIM-SM domain.
ip pim probe-time	Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.
ip pim register-suppress-timeout	Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.

MIB Objects

```

alaPismGlobalConfig
  alaPismV6AdminStatus
  alaPimKeepalivePeriod
  alaPismMaxRPS
  alaPismProbeTime
  alaPimRegisterSuppressionTime
  alaPismV6RPSwitchover
  alaPismV6AdminSPTConfig

```

show ipv6 pim dense

Displays the status of the various global parameters for the IPv6 PIM dense mode.

show ipv6 pim dense

Syntax Definitions

N/A.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show IPv6 pim dense
Status                = enabled,
Source Lifetime       = 210,
State Refresh Interval = 60,
State Refresh Limit Interval = 0,
State Refresh TTL     = 16
```

output definitions

Status	The current global (i.e., switch-wide) status of the IPv6 PIM dense mode. Options include enabled and disabled .
Source Lifetime	The duration of the Keepalive or Source Lifetime timer. The default value is 210.
State Refresh Interval	The time-interval, in seconds, between successive State Refresh messages originated by the router. The default value is 60.
State Refresh Limit Interval	Displays the limit at which a router will not forward the State Refresh messages, if they are received at less than the interval. The default value is 0.
State Refresh TTL	Displays the TTL to be used in the router's originated State Refresh messages. The default value is 16.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim dense admin-state	Enables or disables IPv6 PIM-DM (dense mode) globally on the switch.
ip pim keepalive-period	Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
ip pim state-refresh-interval	Sets the interval between successive State Refresh messages originated by a router.
ip pim state-refresh-limit	Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.
ip pim state-refresh-ttl	Sets the Time to Live to be used in a router's originated State Refresh messages if the data packet's Time to Live is not recorded.

MIB Objects

```
alaPimdmGlobalConfig
  alaPimdmV6AdminStatus
  alaPimKeepalivePeriod
  alaPimRefreshInterval
  alaPimdmStateRefreshLimitInterval
  alaPimdmStateRefreshTimeToLive
```

show ipv6 pim ssm group

Displays the static configuration of IPv6 multicast group mappings for PIM-Source Specific Multicast (SSM).

show ipv6 pim ssm group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim ssm group
```

```
Group Address/Pref Length  Mode  Override Precedence Status
-----+-----+-----+-----+-----
ff00::/8                   ssm   false   none     enabled
ff34::/32                   ssm   false   none     enabled
```

output definitions

Group Address/Pref Length	The IPv6 multicast group address along with the prefix length.
Mode	The IPv6 PIM mode that is used for the groups in this prefix.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that can be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include enabled and disabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 pim ssm group](#)

Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

MIB Objects

```
alaPimStaticRPTable  
  alaPimStaticRPGrpAddress  
  alaPimStaticRPGrpPrefixLength  
  alaPimStaticRPPimMode  
  alaPimStaticRPOverrideDynamic  
  alaPimStaticRPPrecedence  
  alaPimStaticRPRowStatus
```

show ipv6 pim dense group

Displays the static configuration of IPv6 multicast group mappings for PIM Dense Mode (DM).

show ipv6 pim dense group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim dense group
Group Address/Pref Length  Mode  Override  Precedence  Status
-----+-----+-----+-----+-----
ff00::/8                  dm    false    none        enabled
ff34::/32                 dm    false    none        enabled
```

output definitions

Group Address/Pref Length	The IPv6 multicast group address along with the prefix length.
Mode	The IPv6 PIM mode that is used for the groups in this prefix.
Override	Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that can be used for this static RP configuration.
Status	Displays whether this entry is currently enabled or disabled. Options include enabled and disabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 pim dense group](#)

Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

MIB Objects

```
alaPimStaticRPTable
  alaPimStaticRPRowStatus
  alaPimStaticRPGrpPrefixLength
  alaPimStaticRPPimMode
  alaPimStaticRPOverrideDynamic
  alaPimStaticRPPrecedence
  alaPimStaticRPGrpAddress
```

show ipv6 pim interface

Displays detailed IPv6 PIM settings for a specific interface. In general, it displays IPv6 PIM settings for all the interfaces if no argument is specified.

show ipv6 pim interface [*if_name*]

Syntax Definitions

if_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

To view more detailed information about a particular interface, specify the interface name in the command line. Additional information includes Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

Examples

```
-> show ipv6 pim interface
```

Interface Name	Designated Router	Hello Interval	Join/Prune Interval	Oper Status
vlan-5	fe80::2d0:95ff:feac:a537	30	60	enabled
vlan-30	fe80::2d0:95ff:feac:a537	30	60	disabled
vlan-40	fe80::2d0:95ff:fee2:6eec	30	60	enabled

```
-> show ipv6 pim interface vlan-5
```

```
Interface Name           = vlan-5,
IP Address               = fe80::2d0:95ff:fee2:6eec,
Designated Router       = fe80::2d0:95ff:fee2:a537,
Hello Interval          = 30,
Triggered Hello Interval = 5,
Hello HoldTime          = 105,
Join/Prune Interval     = 60,
Join/Prune HoldTime     = 210,
Propagation (Prune) Delay = 500,
Override Interval       = 2500,
Generation ID           = 0x4717be4d,
DR Priority              = 1,
DR Priority Enabled      = true,
Lan Delay Enabled       = true,
Effective Propagation Delay = 500,
Effective Override Interval = 2500,
Suppression Enabled     = true,
Stub Interface          = false,
```

```

Prune Limit Interval      = 60,
Graft Retry Interval     = 3,
State Refresh Enabled    = true,
Operational Status       = enabled

```

output definitions

Interface Name	The name of the IPv6 PIM interface.
IPv6 address	Specifies the IPv6 address of the specified interface.
Designated Router	The primary IP address for the Designated Router (DR). The DR acts on behalf of any directly-connected hosts with respect to the PIM-SM protocol. Only one router in the LAN will act as the DR.
Hello Interval	The frequency at which PIM Hello messages are transmitted on a specified interface. Values may range from 1 to 18000. The default value is 30.
Join/Prune Interval	The Join/Prune interval for the associated interface. The Join/Prune interval is the interval at which periodic PIM-SM Join/Prune messages are sent. Values may range from 0 to 18000. The default value is 60.
Triggered Hello Interval	The current Triggered Hello Interval. This value indicates the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface. Values may range from 0 to 60. The default value is 5.
Hello Holdtime	The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 105.
Join/Prune Holdtime	The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 210.
Propagation Delay	The expected propagation delay between PIM routers on the network. Values may range from 0 to 32767. The default value is 500.
Override Interval	The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.
Generation ID Option	The value of the Generation ID this router inserted in the last PIM Hello message it sent on this interface.
DR Priority	Displays the Designated Router priority for each interface. This value is used in determining the Designated Router on an interface. Values may range from 1 to 192. A higher numeric value denotes a higher priority. Note that priority-based election is used only if all routers on the interface are using the DR priority option. The default value is 1.
Lan Delay Enabled	Options include true and false . The value will be true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting will be false.
Effective Propagation Delay	The Effective Propagation Delay on this interface.

output definitions (continued)

Effective Override Interval	The Effective Override Interval on this interface.
Suppression Enabled	Specifies whether the Join suppression is enabled on this interface.
DR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the DR Priority option.
Stub Interface	Specifies whether this interface is a 'stub interface'. If this is TRUE, then no PIM packets are sent out on this interface, and any received PIM packets are ignored.
Prune Limit Interval	The minimum interval that must transpire between two successive Prunes sent by a router. This is used only with PIM-DM. Values may range from 0 to 65535. The default value is 60.
Graft Retry Interval	Displays the time-interval a router waits for a Graft acknowledgment before resending a Graft on the interface. This is only used with PIM-DM. Values may range from 0 to 65535. The default value is 3.
SR Priority Enabled	Evaluates to TRUE if all routers on this interface are using the State Refresh option. This is used only by PIM-DM.
Operational Status	The current operational status of the corresponding interface. Options include enabled and disabled . This value indicates whether the IPv6 interface is operationally up. For example, if PIM is enabled on the interface, but the interface is currently down, this field will display as disabled. The default setting is disabled . To enable or disable PIM on an interface, refer to the ipv6 pim interface command on page 26-89 . To globally enable or disable PIM on the switch, refer to the ipv6 pim sparse admin-state command on page 26-75 and ipv6 pim dense admin-state command on page 26-76 .

Release History

Release 7.1.1; command was introduced.

Related Commands[ipv6 pim interface](#)

Enables IPv6 PIM and configures statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the interface.

MIB Objects

```
alaPimInterfaceTable
  alaPimInterfaceIfIndex
  alaPimInterfaceDR
  alaPimInterfaceHelloInterval
  alaPimInterfaceJoinPruneInterval
  alaPimInterfaceStatus
  alaPimInterfaceAddress
  alaPimInterfaceTrigHelloInterval
  alaPimInterfaceHelloHoldtime
  alaPimInterfaceJoinPruneHoldtime
  alaPimInterfacePropagationDelay
  alaPimInterfaceOverrideInterval
  alaPimInterfaceGenerationIDValue
```

```
alaPimInterfaceDRPriority  
alaPimInterfaceLanDelayEnabled  
alaPimInterfaceEffectPropagDelay  
alaPimInterfaceEffectOverrideIvl  
alaPimInterfaceSuppressionEnabled  
alaPimInterfaceDRPriorityEnabled  
alaPimInterfaceStubInterface  
AlaPimInterfacePruneLimitInterval  
alaPimInterfaceGraftRetryInterval  
alaPimInterfaceSRPriorityEnabled
```

show ipv6 pim neighbor

Displays a list of active IPv6 PIM neighbors.

show ipv6 pim neighbor [*ipv6_address*] [*if_name*]

Syntax Definitions

ipv6_address The IPv6 address for the PIM neighbor.

if_name The name of the interface.

Defaults

If the neighbor's IPv6 address or interface name is not specified, the entire IPv6 PIM neighbor table is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

To view more detailed information about a particular neighbor, specify the neighbor's IPv6 address or the associated interface name in the command line. Additional information will be displayed, which includes LAN Prune Delay, Override Interval, TBit field, State Refresh capable, and Designated Router option status.

Examples

```
-> show ipv6 pim neighbor
```

Neighbor Address	Interface Name	Uptime	Expires	DR Pri
fe80::2d0:95ff:feac:a537	vlan-30	02h:56m:51s	00h:01m:28s	1

If a specific neighbor address is specified in the command line, *detailed information for the corresponding neighbor only* displays:

```
-> show ipv6 pim neighbor fe80::2d0:95ff:feac:a537
```

```
vlan-30
Neighbor IPv6 Address      = fe80::2d0:95ff:feac:a537,
Uptime                    = 02h:57m:09s,
Expires                   = 00h:01m:40s,
Lan Prune Delay Present   = True,
Propagation Delay         = 500,
Override Interval        = 2500,
TBit Field                = True,
Gen ID Present           = True,
Gen ID Value              = 0x7720c123,
BiDir Capable            = False,
DR Priority Present       = True,
DR Priority               = 1,
```

```

State Refresh Capable      = True,
Secondary Addresses:
  3000::11

vlan-40
Neighbor IPv6 Address      = fe80::2d0:95ff:feac:a537,
Uptime                    = 03h:57m:03s,
Expires                   = 00h:01m:20s,
Lan Prune Delay Present   = True,
Propagation Delay         = 500,
Override Interval         = 2500,
TBit Field                = True,
Gen ID Present            = True,
Gen ID Value              = 0x7720c123,
BiDir Capable             = False,
DR Priority Present        = True,
DR Priority                = 1,
State Refresh Capable     = True,
Secondary Addresses:
  4000::11

```

If a specific interface name is specified in the command line, *detailed information corresponding to all neighbors on the specified interface only* displays:

```

-> show IPv6 pim neighbor vlan-30
vlan-30
Neighbor IPv6 Address      = fe80::2d0:95ff:feac:a537,
Uptime                    = 02h:57m:09s,
Expires                   = 00h:01m:40s,
Lan Prune Delay Present   = True,
Propagation Delay         = 500,
Override Interval         = 2500,
TBit Field                = True,
Gen ID Present            = True,
Gen ID Value              = 0x7720c123,
BiDir Capable             = False,
DR Priority Present        = True,
DR Priority                = 1,
State Refresh Capable     = True,
Secondary Addresses:
  3000::11

```

output definitions

Neighbor IPv6 Address	The IPv6 address of the active PIM neighbor.
Interface Name	The name of the IPv6 PIM interface that is used to reach the neighbor.
Uptime	The amount of time since this PIM neighbor last became a neighbor of the local router, displayed in hours, minutes, and seconds.
Expires	The minimum amount of time remaining before the PIM neighbor will be aged out, displayed in hours, minutes, and seconds.
LAN Prune Delay present	Specifies whether this neighbor is using the LAN Prune Delay option. Options include true or false .
Propagation Delay	The value of the propagation-delay field of the LAN prune-delay option received from this neighbor. A value of 0 indicates that no LAN prune-delay option was received from this neighbor.

output definitions (continued)

Override Interval	The current Override Interval of the LAN prune-delay option received from this neighbor. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by the neighboring router is dictated by this number. Values may range from 0 to 65535. A value of 0 indicates that no LAN prune-delay option was received from this neighbor.
TBit field	The value of the Tbit field of the LAN prune-delay option received from this neighbor. The Tbit specifies the ability of the neighbor to disable Join suppression.
Gen ID present	Specifies whether this neighbor is using Generation ID option. Options include true or false .
Gen ID Value	The value of the Generation ID in the last PIM Hello message received from this neighbor.
BiDir Capable	Specifies whether this neighbor is using the Bidirectional-PIM Capable option.
DR Priority Present	Displays whether the neighbor is using the Designated Router option. Options include true or false .
DR priority	The value of the Designated Router Priority in the last PIM Hello message received from this neighbor.
State Refresh Capable	Displays whether the neighbor is capable of receiving State Refresh messages. Options include true or false .
Secondary Addresses	The secondary IPv6 address of this PIM neighbor.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```

alaPimNeighborTable
  alaPimNeighborAddress
  alaPimNeighborIfIndex
  alaPimNeighborUpTime
  alaPimNeighborExpiryTime
  alaPimNeighborLanPruneDelayPresent
  alaPimNeighborPropagationDelay
  alaPimNeighborTBit
  alaPimNeighborGenerationIDPresent
  alaPimNeighborGenerationIDValue
  alaPimNeighborBiDirCapable
  alaPimNeighborDRPriorityPresent
  alaPimNeighborDRPriority
  alaPimNeighborSRCapable

```



```
alaPimNbrSecAddressTable  
alaPimNbrSecAddress
```

show ipv6 pim static-rp

Displays the IPv6 PIM Static RP table, which includes IPv6 multicast group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the static RP configuration (i.e., enabled or disabled).

```
show ipv6 pim static-rp
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

```
-> show ipv6 pim static-rp
```

Group Address/Pref Length	RP Address	Mode	Override	Precedence	Status
ff00::/8	3000::11	asm	false	none	enabled
ff34::/32	3000::11	asm	false	none	enabled

output definitions

Group Address/Pref Length	The IPv6 multicast group address along with the prefix length.
RP Address	The IPv6 address of the RP that is mapped for the groups within the group prefix. This field is set to zero, if the specified IPv6 PIM mode is SSM or DM.
Mode	The IPv6 PIM mode that is used for the groups in this prefix. The possible values include ASM, SSM, or DM.
Override	Specifies that this static RP configuration can override the dynamically learned RP information for the specified group(s).
Precedence	The precedence value that is used for this static RP configuration.
Status	Displays whether the static RP configuration is currently enabled or disabled. Options include enabled and disabled .

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 pim static-rp](#)

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

MIB Objects

```
alaPimStaticRPTable
  alaPimStaticRPGrpAddress
  alaPimStaticRPGrpPrefixLength
  alaPimStaticRPAddress
  alaPimStaticRPPimMode
  alaPimStaticRPOverrideDynamic
  alaPimStaticRPRowStatus
  alaPimStaticRPPrecedence
```

show ipv6 pim group-map

Displays the IPv6 PIM group mapping table.

show ipv6 pim group-map [**bsr** | **static-rp** | **ssm** | **dense**]

Syntax Definitions

N/A

Defaults

If the keywords **bsr**, **static-rp**, **ssm**, or **dense** are included in the command line, then only the entries that were created by the specified origin are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined through the **ipv6 pim static-rp** command. As long as the RP addresses defined in the static RP set are reachable, they will be added to the group mapping table.
- If the IPv6 multicast groups are mapped to the mode DM or SSM, then the entries created by local SSM address range configuration using the **ipv6 pim ssm group** command and local Dense Mode address range configuration using the **ipv6 pim dense group** command are displayed.
- If the bootstrap mechanism is being used, this information is obtained from received Candidate-RP advertisements (when the local router is the BSR; when the local router is not the BSR, this information is obtained from received bootstrap messages).

Examples

```
-> show ipv6 pim group-map
```

Origin	Group Address/Pref Length	RP Address	Mode	Precedence
BSR	ff00::/8	3000::11	asm	192
BSR	ff00::/8	4000::7	asm	192
SSM	ff33::/32		ssm	

```
-> show ipv6 pim group-map bsr
```

Origin	Group Address/Pref Length	RP Address	Mode	Precedence
BSR	ff00::/8	3000::11	asm	192
BSR	ff00::/8	4000::7	asm	192

```
-> show ipv6 pim group-map ssm
```

Origin	Group Address/Pref Length	RP Address	Mode	Precedence
--------	---------------------------	------------	------	------------

SSM ff33::/32 ssm

output definitions

Origin	The mechanism by which the PIM mode and RP for the group were learned. The possible values include 'static RP' for local static RP configuration, 'static SSM' for both static SSM group configuration and Dense Mode Group configuration, and 'BSR' for the PIM Bootstrap Router mechanism.
Group Address/Prefix Length	The IPv6 multicast group address along with the prefix length.
RP Address	The IPv6 address of the Rendezvous Point to be used for groups within the group prefix.
Mode	The IPv6 PIM mode to be used for groups in this prefix.
Mapping Precedence	The precedence value of a particular row, that determines which row applies to a given group address. Numerically higher values for this object indicate lower precedences, with the value zero denoting the highest precedence.

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 pim static-rp	Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).
ipv6 pim ssm group	Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).
ipv6 pim dense group	Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

MIB Objects

```
alaPimGroupMappingTable
  alaPimGroupMappingOrigin
  alaPimGroupMappingGrpAddress
  alaPimGroupMappingGrpPrefixLength
  alaPimGroupMappingRPAddress
  alaPimGroupMappingPimMode
  alaPimGroupMappingPrecedence
```

show ipv6 pim candidate-rp

Displays the IPv6 multicast groups for which the local router advertises itself as a Candidate-RP.

show ipv6 pim candidate-rp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim candidate-rp
RP Address          Group Address      Priority  Interval  Status
-----+-----+-----+-----+-----
3000::11           FF00::/8           192      60        enabled
```

output definitions

RP Address	An IPv6 unicast address that is advertised as the Candidate-Rendezvous Point (RP).
Group Address	The IPv6 multicast group address along with the prefix length. This is the group for which the local router advertises itself as a C-RP.
Priority	The C-RP router's priority. The lower the value, the higher the priority.
Interval	The time interval at which the C-RP advertisements are sent to the BSR.
Status	The current status of this entry. The status is shown as enabled only if the IPv6 PIM-SM is globally enabled and the IPv6 PIM interface is enabled.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 pim candidate-rp](#)

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IPv6 multicast group(s).

MIB Objects

```
alaPimBsrCandidateRPTable  
  alaPimBsrCandidateRPAddress  
  alaPimBsrCandidateRPGroupAddress  
  alaPimBsrCandidateRPGroupPrefixLength  
  alaPimBsrCandidateRPPriority  
  alaPimBsrCandidateRPInterval  
  alaPimBsrCandidateRPStatus
```

show ipv6 pim cbsr

Displays the IPv6 Candidate-BSR information that is used in the Bootstrap messages.

show ipv6 pim cbsr

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim cbsr
CBSR Address           = 3000::7,
Status                 = enabled,
CBSR Priority          = 0,
Hash Mask Length      = 126,
Elected BSR          = False,
Timer                  = 00h:00m:00s
```

output definitions

CBSR Address	An IPv6 unicast address that the local router uses to advertise itself as a Candidate-BSR.
Status	The current status of this entry. The status is shown as enabled only if the IPv6 PIM-SM is globally enabled and the IPv6 PIM interface is enabled.
CBSR Priority	The value for the local router as a Candidate-BSR. The higher the value, the higher the priority.
Hash Mask Length	The hash mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for an IPv6 multicast group)
Elected BSR	Specifies whether the local router is the elected BSR.
Timer	The time value that is remaining before the local router originates the next Bootstrap message. This value is zero if this router is not the elected BSR.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 pim cbsr](#)

Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBsrCandidateBSRTable  
  alaPimBsrCandidateBSRAddress  
  alaPimBsrCandidateBSRStatus  
  alaPimBsrCandidateBSRHashMaskLength  
  alaPimBsrCandidateBSRElectedBSR  
  alaPimBsrCandidateBSRBootstrapTimer  
  alaPimBsrCandidateBSRPriority
```

show ipv6 pim bsr

Displays information about the elected IPv6 BSR.

```
show ipv6 pim bsr
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim bsr
BSR Address           = 3000::7,
BSR Priority           = 192,
Hash Mask Length      = 126,
Expiry Time           = 00h:01m:35s
```

output definitions

BSR Address	The IPv6 unicast address of the elected BSR.
BSR Priority	The priority value of the elected BSR. The higher the value, the higher the priority.
Hash Mask Length	The hash mask length that is advertised in the Bootstrap messages by the elected BSR (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group).
Expiry Time	The minimum time remaining before the elected BSR will be declared down.

Release History

Release 7.1.1; command was introduced.

Related Commands

[ipv6 pim cbsr](#)

Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```
alaPimBsrElectedBSRTable  
  alaPimBsrElectedBSRAddress  
  alaPimBsrElectedBSRPriority  
  alaPimBsrElectedBSRHashMaskLength  
  alaPimBsrElectedBSRExpiryTime
```

show ipv6 pim groute

Displays all (*,G) state that the IPv6 PIM has.

```
show ipv6 pim groute [group_address]
```

Syntax Definitions

group_address The IPv6 address of the Multicast Group.

Defaults

By default, entire (*,G) routing table is displayed. To view more detailed (*,G) state information about a particular group, specify the group address in the command line.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When the *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.

Examples

```
-> show ipv6 pim groute
Total 1 (*,G)
```

Group Address	RP Address	RPF Interface	UpTime
ff0e::7	5ffe::3	vlan-4	00h:01m:23s

```
-> show ipv6 pim groute ff0e::7
(*,ff0e::7)
  UpTime                = 00h:01m:28s
  RP Address             = 5ffe::3,
  PIM Mode               = ASM,
  PIM Mode Origin       = BSR,
  Upstream Join State   = Not Joined,
  Upstream Join Timer   = 00h:00m:00s,
  Upstream Neighbor     = fe80::220:fcff:fe1e:2455,
  RPF Interface         = vlan-4,
  RPF Next Hop          = fe80::220:fcff:fe1e:2455,
  RPF Route Protocol    = Static,
  RPF Route Address     = 5ffe::3/128,
  RPF Route Metric Pref = 10,
  RPF Route Metric      = 10,
  Interface Specific State:
    vlan-3
      UpTime              = 00h:01m:28s,
      Local Membership    = False,
      Join/Prune State    = Joined,
      Prune Pending Timer = 00h:00m:00s,
```

```

Join Expiry Timer      = 00h:02m:02s,
Assert State          = Loser,
Assert Timer          = 00h:01m:32s,
Assert Winner Address = fe80::220:fcff:fe1e:2454,
Assert Winner Metric Pref = 9 (rpt),
Assert Winner Metric  = 10,
vlan-4
UpTime                = 00h:00m:00s,
Local Membership      = False,
Join/Prune State      = No Info,
Prune Pending Timer   = 00h:00m:00s,
Join Expiry Timer     = 00h:00m:00s,
Assert State          = No Info,
Assert Timer          = 00h:00m:00s,
vlan-5
UpTime                = 00h:00m:00s,
Local Membership      = False,
Join/Prune State      = No Info,
Prune Pending Timer   = 00h:00m:00s,
Join Expiry Timer     = 00h:00m:00s,
Assert State          = No Info,
Assert Timer          = 00h:00m:00s,

```

output definitions

Group-address	The IPv6 Multicast Group Address.
RP Address	The address of the Rendezvous Point (RP) for the group.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (*,G) join messages to.
UpTime	The time since this entry was created.
Pim Mode Origin	The mechanism by which the PIM mode and RP for the group were learned.
Upstream Join State	Whether the local router should join the RP tree for the group.
Upstream Join Timer	The time remaining before the local router next sends a periodic (*,G) Join message on the RPF IfIndex.
RPF Next Hop	The address of the RPF next hop towards the RP.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF interface towards the RP was learned.
RPF Route Address/Prefix Length	The IPv6 address combined with the prefix length identifies the route used to find the RPF interface towards the RP.
Route Metric Pref	The metric preference of the route used to find the RPF interface towards the RP.
Route Metric	The routing metric of the route used to find the RPF interface towards the RP.
Interface Name	The interface name that corresponds to the ifIndex.
Local Membership	Whether the local router has (*,G) local membership on this interface.
Join Prune State	The state resulting from (*,G) Join/Prune messages received on this interface.

output definitions (continued)

Prune Pending Timer	The time remaining before the local router acts on a (*,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.
Join Expiry Timer	The time remaining before (*,G) Join state for this interface expires.
Assert State	The (*,G) Assert state for this interface. The possible values are No Info, Winner or Loser.
Assert Timer	If Assert State is 'Winner', this is the time remaining before the local router next sends a (*,G) Assert message on this interface. If the Assert State is 'Loser', this is the time remaining before the (*,G) assert state expires.
Assert Winner Address	If the Assert State is 'Loser', this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is 'Loser', this is the metric preference of the route to the RP advertised by the assert winner; otherwise, this is zero.
Assert Winner Metric	If the Assert State is 'Loser', this is the routing metric of the route to the RP advertised by the assert winner; otherwise, this is zero.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

alaPimStarGTable

```

alaPimStarGGrpAddress
alaPimStarGRPAddress
alaPimStarGRPFIfIndex
alaPimStarGUpstreamNeighbor
alaPimStarGUpTime
alaPimStarGPimModeOrigin
alaPimStarGUpstreamJoinState
alaPimStarGUpstreamJoinTimer
alaPimStarGRPFNextHop
alaPimStarGRPFRouteProtocol
alaPimStarGRPFRouteAddress
alaPimStarGRPFRoutePrefixLength
alaPimStarGRPFRouteMetricPref
alaPimStarGRPFRouteMetric

```

alaPimStarGITable

```

alaPimStarGIIfIndex
alaPimStarGILocalMembership
alaPimStarGIJoinPruneState
alaPimStarGIPrunePendingTimer
alaPimStarGIPrunePendingTimer
alaPimStarGIAssertState
alaPimStarGIAssertTimer
alaPimStarGIAssertWinnerAddress
alaPimStarGIAssertWinnerAddress

```

alaPimStarGIAssertWinnerMetric

show ipv6 pim sgroute

Displays all (S,G) state that the IPv6 PIM has.

show ipv6 pim sgroute [*source_address* *group_address*]

Syntax Definitions

source_address The IPv6 address for a specific multicast source.

group_address A IPv6 multicast address.

Defaults

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the *source_address* and *group_address* associated with that entry.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When the *source_address* and *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IPv6 address is not specified, the current PIM status for all multicast route entries are displayed.

Examples

```
-> show ipv6 pim sgroute
```

```
Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
           L = Local, R = RPT, T = SPT, F = Register,
           P = Pruned, O = Originator
```

```
Total 1 (S,G)
```

Source Address	Group Address	RPF Interface	UpTime	Flags
8ffe::3	ff0e::7		00h:01m:34s	SR

```
-> show ipv6 pim sgroute 8ffe::3 ff0e::7
(8ffe::3,ff0e::7)
```

```
UpTime                                = 00h:01m:40s
PIM Mode                              = ASM,
Upstream Join State                   = Not Joined,
Upstream RPT State                   = Not Pruned,
Upstream Join Timer                   = 00h:00m:00s,
Upstream Neighbor                    = none,
SPT Bit                                = False,
DR Register State                     = No Info,
DR Register Stop Timer                = 00h:00m:00s,
Interface Specific State:
```



```

vlan-3
  UpTime                = 00h:01m:40s,
  Local Membership      = False,
  Join/Prune State      = No Info,
  RPT State             = No Info,
  Prune Pending Timer   = 00h:00m:00s,
  Join Expiry Timer     = 00h:00m:00s,
  Assert State         = No Info,
  Assert Timer          = 00h:00m:00s,
vlan-4
  UpTime                = 00h:00m:00s,
  Local Membership      = False,
  Join/Prune State      = No Info,
  RPT State             = No Info,
  Prune Pending Timer   = 00h:00m:00s,
  Join Expiry Timer     = 00h:00m:00s,
  Assert State         = No Info,
  Assert Timer          = 00h:00m:00s,
vlan-5
  UpTime                = 00h:00m:00s,
  Local Membership      = False,
  Join/Prune State      = No Info,
  RPT State             = No Info,
  Prune Pending Timer   = 00h:00m:00s,
  Join Expiry Timer     = 00h:00m:00s,
  Assert State         = No Info,
  Assert Timer          = 00h:00m:00s,

```

output definitions

Source-address	The IPv6 Source address.
Group-address	The IPv6 Multicast Group Address.
RPF Interface	The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.
Upstream Neighbor	The primary address of the neighbor on the RPF Interface that the local router is sending periodic (S,G) join messages to.
UpTime	The time since this entry was created.
Flags	Flags indicating SPTBit, Prune State, Join State, etc.
Pim Mode	Whether the Group Address is SSM, ASM or DM.
Upstream Join State	Whether the local router should join the SPT for the source and group represented by this entry.
Upstream Join Timer	The time remaining before the local router next sends a periodic (S,G) Join message.
RPF Next Hop	The address of the RPF next hop towards the source.
RPF Route Protocol	The routing mechanism through which the route used to find the RPF Interface towards the source was learned.
RPF Route Address/Prefix Length	The IP address which when combined with the Route Prefix length identifies the route used to find the RPF interface towards the source.
RPF Route Metric Pref	The metric preference of the route used to find the RPF interface towards the source.

output definitions (continued)

RPF Route Metric	The metric preference of the route used to find the RPF interface towards the source.
DR Register State	Whether the local router should encapsulate (S,G) data packets in Register messages and send them to the RP. The possible values include No Info, Join, Join Pending, or Prune.
DR Register Stop Timer	The value of the Register Stop Timer. If the Register State is 'prune', this is the time remaining before the local router sends a Null-Register message to the RP. If the State is 'joinPending', this is the time remaining before the local router resumes encapsulating data packets and sending them to the RP.
Upstream Prune State	Whether the local router has pruned itself from the tree. This is only used by PIM-DM. The possible values include forwarding, Ack Pending, or Pruned.
Upstream Prune Limit Timer	The time remaining before the local router may send a (S,G) prune message on alaPimSGRPFIfIndex. This is only used by PIM-DM.
Originator State	Whether this router is an originator for the (S,G) message flow. This is only used by PIM-DM. The possible values include Not Originator or Originator.
Source Active Timer	If this router is the Originator, this is the time remaining before the local router reverts to notOriginator state. Otherwise, this is zero. This is only used by PIM-DM.
State Refresh Timer	If Originator state is 'originator', this is the time remaining before the local router sends a State Refresh Message. Otherwise, this is zero. This is only used by PIM-DM.
Interface Name	The interface name corresponding to the ifIndex that corresponds to this entry.
Uptime	The time since this entry was created.
Local Membership	Whether the local router has (S,G) local membership on this interface.
Join Prune State	The state resulting from (S,G) Join/Prune messages received on this interface. The possible values include No Info, Join, or Prune Pending.
Prune Pending Timer	The time remaining before the local router acts on an (S,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.
Join Expiry Timer	The time remaining before (S,G) Join state for this interface expires.
Assert State	The (S,G) Assert state for this interface. The possible values include No Info, Winner, or Loser.
Assert Timer	If Assert State is Winner, this is the time remaining before the local router sends a (S,G) Assert message on this interface. If the Assert State is Loser, this is the time remaining before the (S,G) Assert state expires.
Assert Winner	If the Assert State is Loser, this is the address of the assert winner.
Assert Winner Metric Pref	If the Assert State is Loser, this is the metric preference of the route to the source advertised by the assert winner.
Assert Winner Metric Metric	If the Assert State is Loser, this is the routing metric of the route to the source advertised by the assert winner.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

alaPimSGTable

- alaPimSGSrcAddress
- alaPimSGGrpAddress
- alaPimSGRPFIfIndex
- alaPimSGUpstreamNeighbor
- alaPimSGUpTime
- alaPimSGSPTBit
- alaPimSGUpstreamPruneState
- alaPimSGUpstreamJoinState
- alaPimSGPimMode
- alaPimSGUpstreamJoinState
- alaPimSGUpstreamJoinTimer
- alaPimSGRPFNextHop
- alaPimSGRPFRouteProtocol
- alaPimSGRPFRouteAddress
- alaPimSGRPFRoutePrefixLength
- alaPimSGRPFRouteMetricPref
- alaPimSGRPFRouteMetric
- alaPimSGDRRegisterState
- alaPimSGDRRegisterStopTimer
- alaPimSGUpstreamPruneState
- alaPimSGUpstreamPruneLimitTimer
- alaPimSGOriginatorState
- alaPimSGSourceActiveTimer
- alaPimSGStateRefreshTimer

alaPimSGITable

- alaPimSGIIfIndex
- alaPimSGIUpTime
- alaPimSGILocalMembership
- alaPimSGIJoinPruneState
- alaPimSGIPrunePendingTimer
- alaPimSGIJoinExpiryTimer
- alaPimSGIAssertState
- alaPimSGIAssertTimer
- alaPimSGIAssertWinnerAddress
- alaPimSGIAssertWinnerMetricPref
- alaPimSGIAssertWinnerMetric

27 Multicast Routing Commands

This chapter describes multicast routing commands. Multicast routing is used in conjunction with IP Multicast Switching (IPMS). IPMS can operate either with or without multicast routing. However, for Multicast Routing to function, IPMS must be configured.

Multicast uses Class D IP addresses in the range 224.0.0.0 to 239.255.255.255. Addresses in the range 239.0.0.0 to 239.255.255.255 are reserved for boundaries, which are used to prevent multicast traffic from being forwarded on a VLAN group or network.

IP multicast routing is a way of controlling multicast traffic across networks. The multicast router discovers which networks want to receive multicast traffic by sending out Internet Group Management Protocol (IGMP) queries and receiving IGMP reports from attached networks. The IGMP reports signal that users want to join or leave a multicast group. If there is more than one multicast router in the network, the router with the lowest IP address is elected the querier router, which is responsible for querying the subnetwork for group members.

The current release also provides support for IPv6 multicast addresses. In the IPv6 addressing scheme, multicast addresses begin with the prefix ff00::/8. Similar to IPv6 unicast addresses, IPv6 multicast addresses also have different scopes depending on their prefix, though the range of possible scopes is different.

Multicast Listener Discovery (MLD) is the protocol used by an IPv6 router to discover the nodes which request multicast packets on its directly attached links and the multicast addresses that are of interest to those neighboring nodes. MLD is derived from version 2 of IPv4's Internet Group Management Protocol, IGMPv2. MLD uses ICMPv6 message types, rather than IGMP message types.

MIB information for the multicast routing commands is as follows:

Filename: AlcatelIND1Ipmmr.mib
Module: ALCATEL-IND1-IPMRM-MIB

Filename: AlcatelIND1IpMcastDraft.mib
Module: ALCATEL-IND1-IPMCAST-MIB

A summary of the available commands is listed here:

ip mroute-boundary
ip mroute interface ttl
ipv6 mroute interface ttl
show ip mroute-boundary
show ip mroute
show ipv6 mroute
show ip mroute interface
show ipv6 mroute interface
show ip mroute-nexthop
show ipv6 mroute-nexthop

ip mroute-boundary

Adds or deletes scoped multicast address boundaries for a router interface. When a user on the specified interface joins the multicast group as defined by the scoped address—plus the mask length—all multicast traffic will stop being forwarded on that interface. This provides a mechanism for the end user to control multicast traffic from the network.

Refer to the “Configuring Multicast Address Boundaries” chapter in the applicable *OmniSwitch Advanced Routing Guide* for detailed information.

ip mroute-boundary *if_name scoped_address mask*

no ip mroute-boundary *if_name scoped_address mask*

Syntax Definitions

<i>if_name</i>	The interface name on which the boundary is being assigned.
<i>scoped_address</i>	A scoped multicast address identifying the group range for the boundary. Scoped addresses may range from 239.0.0.0–239.255.255.255.
<i>mask</i>	A corresponding Class A, B, or C mask address (e.g., 255.0.0.0).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to delete the scoped multicast address boundaries for a router interface.

Examples

```
-> ip mroute-boundary vlan-2 239.0.0.0 255.0.0.0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip mroute-boundary Displays scoped multicast address boundaries for the switch’s router interfaces.

MIB Objects

IpMRouteBoundaryTable

 ipMRouteBoundaryIfIndex

 ipMRouteBoundaryAddress

 ipMRouteBoundaryAddressMask

 ipMRouteBoundaryStatus

ip mroute interface ttl

Specifies a multicast datagram Time to Live (TTL) threshold for an existing router interface. IP multicast datagrams with a TTL value lower than the specified TTL threshold value will not be forwarded out of the interface.

ip mroute interface *if_name* **ttl** *threshold*

Syntax Definitions

<i>if_name</i>	The interface name that has one of the Multicast routing protocols running (either DVMRP or PIM).
<i>threshold</i>	The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded out of the interface.

Defaults

parameter	default
<i>threshold</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ip mroute interface vlan-1 ttl 255
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip mroute interface](#) Displays IP multicast interface information.

MIB Objects

```
alaIpMcastInterfaceTable  
  alaIpMcastInterfaceIfIndex  
  alaIpMcastInterfaceTtl
```

ipv6 mroute interface ttl

Specifies a multicast datagram Time to Live (TTL) threshold for an existing IPv6 interface. Any IP multicast datagrams with a TTL value lower than the specified TTL threshold value will not be forwarded out of the interface.

ipv6 mroute interface *if_name* **ttl** *threshold*

Syntax Definitions

<i>if_name</i>	The name of the IPv6 interface.
<i>threshold</i>	The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded out of the interface.

Defaults

parameter	default
<i>threshold</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ipv6 mroute interface vlan-1 ttl 255
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ipv6 mroute interface](#) Displays IPv6 multicast interface information.

MIB Objects

```
alaIpMcastInterfaceTable  
  alaIpMcastInterfaceIfIndex  
  alaIpMcastInterfaceTtl
```

show ip mroute-boundary

Displays scoped multicast address boundaries for the switch's router interfaces.

show ip mroute-boundary

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip mroute-boundary
```

```
Interface Name  Interface Address  Boundary Address
-----+-----+-----
vlan-4          214.0.0.7          239.1.1.1/32
```

output definitions

Interface Name	The name of the interface on which the boundary is assigned. Packets with a destination address in the associated address/mask range will not be forwarded from this interface.
Interface Address	The IP address of this interface where the boundary is assigned.
Boundary Address	The scoped multicast address that, when combined with the boundary mask, identifies the scoped boundary range. The boundary's subnet mask is shown using the CIDR prefix length: 255.0.0.0 equals /8; 255.255.0.0 equals /16; 255.255.255.0 equals /24.

Release History

Release 7.1.1; command was introduced.

Related Commands

ip mroute-boundary Adds or deletes a router's scoped multicast address boundaries.

MIB Objects

IpMRouteBoundaryTable
 ipMRouteBoundaryIfIndex
 ipMRouteBoundaryAddress
 ipMRouteBoundaryAddressMask
 ipMRouteBoundaryStatus

show ip mroute

Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

show ip mroute

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

-> show ip mroute

```
Total 2 Mroutes
Group Address      Src Address      Upstream Nbr      Route Address      Proto
-----+-----+-----+-----+-----
225.0.0.0          214.0.0.2/32    0.0.0.0           214.0.0.0/24      PIM-SM
225.0.0.1          214.0.0.2/32    0.0.0.0           214.0.0.0/24      PIM-DM
```

output definitions

Group Address	The IP multicast group address for this entry.
Src Address	The network address which identifies the source for this entry.
Upstream Nbr	The address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received.
Route Address	The address portion of the route used to find the upstream or parent interface for this multicast forwarding entry.
Proto	The multicast routing protocol through which this multicast forwarding entry was learned (i.e., DVMRP, PIM-SM or PIM-DM).

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastRouteTable
  alaIpMcastRouteGroup
  alaIpMcastRouteSource
  alaIpMcastRouteInIfIndex
  alaIpMcastRouteUpstreamNeighbor
  alaIpMcastRouteRtAddress
  alaIpMcastRouteRtPrefixLength
  alaIpMcastRouteProtocol
```

show ipv6 mroute

Displays multicast routing information for IPv6 datagrams sent by particular sources to the IPv6 multicast groups known to this router.

show ipv6 mroute

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 mroute
Total 2 Mroutes
Group Address Source Address Interface Upstream Neighbor Route Addr/Prefix Len
Proto
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
ff06:7777::1 2600::7      vlan-30  fe80::2d0:95ff:feac:a537 2600::/64
PIM-SM
ff06:7777::2 2600::7      vlan-30  fe80::2d0:95ff:feac:a537 2600::/64
PIM-SM
```

output definitions

Group Address	The IPv6 multicast group address for this entry.
Source Address	The IPv6 multicast address, which identifies the source for this entry.
Interface	The name of the IPv6 interface on which the datagrams sent by these sources to this IPv6 multicast address are received.
Upstream Neighbor	The IPv6 address of the upstream neighbor from which the datagrams from these sources to this multicast address are received.
Route Addr/Prefix len	The IPv6 address portion of the route used to find the upstream or parent interface for this IPv6 multicast forwarding entry.
Proto	The IPv6 multicast routing protocol through which this IPv6 multicast forwarding entry was learned.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastRouteTable
  alaIpMcastRouteGroup
  alaIpMcastRouteSource
  alaIpMcastRouteInIfIndex
  alaIpMcastRouteUpstreamNeighbor
  alaIpMcastRouteRtAddress
  alaIpMcastRouteRtPrefixLength
  alaIpMcastRouteProtocol
```

show ip mroute interface

Displays IP multicast interface information.

show ip mroute interface {*interface_name*}

Syntax Definitions

interface_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Not specifying an interface name displays all known IP multicast interfaces information.

Examples

-> show ip mroute interface

Interface Name	IP Address	TTL	Multicast Protocol
vlan-4	214.0.0.7	0	PIM
vlan-26	172.21.63.7	0	PIM
vlan-11	212.61.11.7	0	PIM

output definitions

Interface Name	The name configured for the interface.
IP Address	The IP address of this interface entry.
TTL	The datagram TTL threshold for the interface. Any IP multicast datagrams with a TTL less than the threshold displayed in the table will not be forwarded out of the interface. The default value, 0, specifies that <i>all</i> multicast packets are forwarded out of the interface.
Multicast Protocol	The multicast routing protocol currently running on this interface. Options include DVMRP and PIM.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastInterfaceTable  
  alaIpMcastInterfaceIfIndex  
  alaIpMcastInterfaceTtl  
  alaIpMcastInterfaceProtocol
```

show ipv6 mroute interface

Displays IPv6 multicast interface information.

show ipv6 mroute interface *{interface_name}*

Syntax Definitions

interface_name The name of the interface.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Not specifying an interface name displays all known IPv6 multicast interfaces information.

Examples

-> show ipv6 mroute interface

Interface Name	IP Address	TTL	Multicast Protocol
vlan-4	2000::1	0	PIM
vlan-26	2000::2	0	PIM
vlan-11	2000::3	0	PIM

output definitions

Interface Name	The name configured for the IPv6 interface.
IP Address	The IPv6 address of this interface entry.
TTL	The datagram TTL threshold for the interface. Any IPv6 multicast datagrams with a TTL less than the threshold displayed in the table will not be forwarded out of the interface. The default value, 0, specifies that <i>all</i> multicast packets are forwarded out of the interface.
Multicast Protocol	The multicast routing protocol currently running on this interface. Options include DVMRP and PIM.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastInterfaceTable  
  alaIpMcastInterfaceIfIndex  
  alaIpMcastInterfaceTtl  
  alaIpMcastInterfaceProtocol
```

show ip mroute-nexthop

Displays next-hop information on outgoing interfaces for routing IP multicast datagrams.

show ip mroute-nexthop

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ip mroute-nexthop
```

```
Total 10 Nexthops
```

Group Address	Src Address	Interface Name	Next Hop Address	Protocol
225.0.0.0	214.0.0.2/32	vlan-26	225.0.0.0	PIM-SM
225.0.0.1	214.0.0.2/32	vlan-26	225.0.0.1	PIM-SM
225.0.0.2	214.0.0.2/32	vlan-26	225.0.0.2	PIM-SM
225.0.0.3	214.0.0.2/32	vlan-26	225.0.0.3	PIM-SM
225.0.0.4	214.0.0.2/32	vlan-26	225.0.0.4	PIM-SM
225.0.0.5	214.0.0.2/32	vlan-26	225.0.0.5	PIM-SM
225.0.0.6	214.0.0.2/32	vlan-26	225.0.0.6	PIM-SM
225.0.0.7	214.0.0.2/32	vlan-26	225.0.0.7	PIM-SM
225.0.0.8	214.0.0.2/32	vlan-26	225.0.0.8	PIM-SM
225.0.0.9	214.0.0.2/32	vlan-26	225.0.0.9	PIM-SM

output definitions

Group Address	The IP multicast group address for this entry.
Src Address	The network address, which identifies the source for this entry.
Interface Name	Generally, this is the name configured for the interface.
Next Hop Address	The address of the next-hop that is specific to this entry.
Protocol	The routing protocol by which this next-hop was learned (i.e., DVMRP or PIM-SM).

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ip mroute](#)

Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

MIB Objects

```
alaIpMcastRouteNextHopTable
  alaIpMcastRouteNextHopGroup
  alaIpMcastRouteNextHopSource
  alaIpMcastRouteNextHopIfIndex
  alaIpMcastRouteNextHopAddress
  alaIpMcastRouteNextHopProtocol
```

show ipv6 mroute-nexthop

Displays IPv6 next-hop information on outgoing interfaces for routing IP multicast datagrams.

show ipv6 mroute-nexthop

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ipv6 mroute-nexthop
```

```
Total 2 Nexthops
```

Group Address	Source Address	Interface	Next Hop Address	Protocol
ff06:7777::1	2600::7	vlan-40	ff06:7777::1	PIM-SM
ff06:7777::2	2600::7	vlan-40	ff06:7777::2	PIM-SM

output definitions

Group Address	The IPv6 multicast group address for this entry.
Src Address	The IPv6 multicast address, which identifies the source for this entry.
Interface Name	The name of the IPv6 interface on which the datagrams sent by these sources to this IPv6 multicast address are received.
Next Hop Address	The IPv6 address of the next-hop that is specific to this entry.
Protocol	The IPv6 multicast routing protocol by which this IPv6 multicast forwarding entry was learned.

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

```
alaIpMcastRouteNextHopTable  
  alaIpMcastRouteNextHopGroup  
  alaIpMcastRouteNextHopSource  
  alaIpMcastRouteNextHopIfIndex  
  alaIpMcastRouteNextHopAddress  
  alaIpMcastRouteNextHopProtocol
```

28 QoS Commands

Alcatel-Lucent's QoS software provides a way to manipulate flows coming through the switch based on user-configured policies. The flow manipulation (generally referred to as *Quality of Service* or *QoS*) may be as simple as allowing/denying traffic, or as complicated as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

This chapter provides information about configuring QoS global and port parameters through the Command Line Interface (CLI). Refer to [Chapter 44, "QoS Policy Commands,"](#) for information about commands used to configure QoS policy rules.

MIB information for the QoS commands is as follows:

Filename: ALCATEL-IND1-QOS-MIB_mib
Module alaQoS MIB

Filename: ALCATEL-IND1-VIRTUAL-FLOW-CONTROL-MIB_mib
Module alcatelIND1VfcMIB

Important Note. Some of the commands listed here are not currently supported on one or more platforms. See command descriptions in this chapter and check release notes for information about commands that are not supported.

The QoS commands are listed here:

Global commands	qos qos trust-ports qos forward log qos log console qos log lines qos log level qos stats interval qos phones qos user-port qos dei debug qos debug qos internal clear qos log qos apply qos revert qos flush qos reset qos stats reset show qos slice show qos log show qos config show qos statistics
------------------------	--

Port and Slice commands	<code>qos port</code> <code>qos port reset</code> <code>qos port trusted</code> <code>qos port maximum egress-bandwidth</code> <code>qos port maximum ingress-bandwidth</code> <code>qos port default 802.1p</code> <code>qos port default dscp</code> <code>qos port default classification</code> <code>qos port dei</code> <code>show qos port</code>
Queue Management commands	<code>qos qsi qsp</code> <code>qos qsi wred</code> <code>qos qsi stats</code> <code>show qos wrp</code> <code>show qos qsp</code> <code>show qos qsi</code> <code>show qos qsi stats</code> <code>show qos qsi stats rate</code> <code>show qos qsi stats bytes</code> <code>show qos qsi wred-stats</code> <code>clear qos qsi stats</code>
Data Center Bridging commands	<code>qos qsp dcb import</code> <code>qos qsp dcb tc</code> <code>qos qsp dcb tc-numbering</code> <code>qos qsi qsp dcb</code> <code>qos qsi dcb dcbx admin-state</code> <code>qos qsi dcb dcbx ets</code> <code>qos qsi dcb dcbx pfc</code> <code>qos qsi stats admin-state</code> <code>show qos qsp dcb</code> <code>show qos qsi dcbx</code> <code>show qos qsi summary</code> <code>show qos qsi dcb ets</code> <code>show qos qsi dcbx pfc</code> <code>show qos pfc-lossless-usage</code> <code>show qos qsi dcb pfc stats</code> <code>show qos qsi stats</code> <code>clear qos qsi dcb pfc stats</code>

qos

Enables or disables QoS. This section describes the base command with a single required option (**enable** or **disable**).

In lieu of these options, the base command (**qos**) may be used with other keywords to set up global QoS configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

```
qos {enable | disable}
    [trust-ports]
    [forward log]
    [log console]
    [log lines lines]
    [log level level]
    [stats interval seconds]
    [phones [priority priority_value | trusted]]
    [user-port {filter | shutdown} {snoop | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcpserver
    | dns-reply}]
```

Syntax Definitions

enable	Enables QoS. The QoS software in the switch classifies flows coming into the switch to attempt to match them to QoS policies. If a match is found, the policy parameters are applied to the flow. The enable setting may be used alone or in conjunction with optional command keywords.
disable	Disables QoS. Flows coming into the switch are not matched to policies. The disable setting cannot be used with any other command keyword.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When QoS is disabled, flows coming into the switch are classified but not matched to a policy. Traffic is treated as best effort and assigned to default queues.
- The command keywords may be used with or without **enable**; these keywords cannot be used with **disable**.

Examples

```
-> qos enable default disposition deny
```

```
-> qos disable  
-> qos enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy rule	Configures a policy rule on the switch.
show policy rule	Displays information for policy rules configured on the switch.

MIB Objects

```
alaQoSConfigTable  
  alaQoSConfigEnable  
  alaQoSConfigTrustedPorts  
  alaQoSConfigForwardLog  
  alaQoSConfigLogLines  
  alaQoSConfigLogLevel  
  alaQoSConfigLogConsole  
  alaQoSConfigStatsInterval  
  alaQoSConfigAutoPhones  
  alaQoSConfigUserportFilter  
  alaQoSConfigAppliedUserportFilter  
  alaQoSConfigUserportShutdown  
  alaQoSConfigAppliedUserportShutdown
```

qos trust-ports

Configures the global trust mode for QoS ports. Trusted ports can accept 802.1p and ToS/DSCP values in incoming packets; untrusted ports will set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured.

Any port configured through the **qos port** command will automatically be added in the trust mode specified by this command. See [page 28-32](#) for more information about this command.

qos trust-ports

qos no trust-ports

Syntax Definitions

N/A

Defaults

By default, all ports are untrusted.

Platforms Supported

OmniSwitch 10K, 6900

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 are always trusted regardless of the global setting.
- Use the **qos port default 802.1p** or **qos port default dscp** commands to specify that a value other than zero should be applied to the incoming packets. Note that this value is overridden if a policy exists that specifies a different value for such packets.

Examples

```
-> qos trust-ports  
-> qos no trust-ports
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port trusted	Configures whether or not a particular port is trusted or untrusted.
show qos port	Displays information about QoS ports.

MIB Objects

alaQoSConfigTable
 alaQoSConfigTrustedPorts

qos forward log

Enables the QoS software in the switch to send events to the policy server software in the switch in real time. The policy server software may then be polled by an NMS application for logged events.

qos forward log

qos no forward log

Syntax Definitions

N/A

Defaults

By default, logged events are not sent to the policy server software in the switch.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

An NMS application may query the Policy Manager in the switch for logged events. Use the **qos forward log** command to forward each event as it happens.

Examples

```
-> qos forward log
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable  
  alaQoSConfigForwardLog
```

qos log console

Sends QoS log messages to the switch logging utility, which is an event logging application available on the OmniSwitch. The configuration of the switch logging utility determines if QoS messages are sent to a log file in the switch's flash file system, displayed on the switch console, or sent to a remote syslog server.

qos log console

qos no log console

Syntax Definitions

N/A

Defaults

QoS log messages are not sent to the switch logging utility by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- To display QoS log events as they happen on an output console attached to the switch, configure the switch logging utility to output events to the console. This is done using the **swlog output** command.
- The entire log may be viewed at any time using the **show qos log** command.

Examples

```
-> qos log console
-> qos no log console
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
swlog output	Enables or disables switch logging output to the console, file, or data socket (remote session).
swlog output	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
<i>lines</i>	10000

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- To turn off logging, enter 0 for the number of log lines. (Note that error messages will still be logged.)
- If you change the number of log lines, you may clear all messages in the QoS log. To avoid clearing all messages in the log, enter the **qos log lines** command in the **boot.cfg** file. The log length will be changed at the next reboot.

Examples

```
-> qos log lines 5  
-> qos log lines 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show qos log](#) Displays the log of QoS events.

MIB Objects

alaQoSConfigTable
 alaQoSConfigLogLines

qos log level

Configures the level of log detail.

qos log level *level*

qos no log level

Syntax Definitions

level The level of log detail, in the range from 1 (least detail) to 8 (most detail).

Defaults

parameter	default
<i>level</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **qos debug** command to change the type of debugging messages that are logged. The **qos log level** command configures the level of detail for these messages.
- If the **qos debug** command is not configured to log any kind of information (this is the default), the **qos log level** command has no effect.
- To log fatal errors only, set the log level to 0.
- Note that a high log level value will impact the performance of the switch.

Examples

```
-> qos log level 4  
-> qos log level 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands**qos log lines**

Configures the number of lines in the QoS log.

show qos log

Displays the log of QoS events.

MIB Objects

alaQoSConfigTable

 alaQoSConfigLogLevel

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 1–3600.

Defaults

parameter	default
<i>seconds</i>	60

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show qos statistics](#)

Displays statistics about the QoS configuration.

MIB Objects

alaQoSConfigTable

alaQoSConfigStatsInterval

qos phones

Enables or disables the automatic prioritization of IP phone traffic.

qos phones [*priority* *priority_value* | **trusted**]

qos no phones

Syntax Definitions

priority_value The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).

trusted Trusts IP phone traffic; priority value of the IP phone packet is used.

Defaults

parameter	default
<i>priority_value</i> trusted	trusted

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable automatic prioritization of IP phone traffic.
- IP phone traffic is identified by examining the source MAC address of the packet received on the port. If the source MAC falls within one of the following ranges, the QoS IP phone priority is automatically assigned to the MAC:
 00-80-9F-54-xx-xx to 00-80-9F-64-xx-xx
 00-80-9F-66-xx-xx to 00-80-9F-6F-xx-xx.
- To automatically apply the QoS IP phone priority to other, non-IP phone traffic, add the source MAC addresses of such traffic to the QoS “alaPhone” group.
- When automatic prioritization of IP phone traffic is enabled, QoS policies that specify priority are not applied to the IP phone traffic. Other QoS policies, however, are applied to this type of traffic as usual.

Examples

```
-> qos phones priority 7
-> qos phones trusted
-> qos no phones
```

Release History

Release 7.1.1; command was 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 | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}
```

```
qos no user-port {filter | shutdown}
```

Syntax Definitions

filter	Filters the specified type of traffic when it is received on UserPort ports.
shutdown	Administratively disables UserPort ports that receive the specified type of traffic.
spoof	Detects IP spoofing. The source IP address of a packet ingressing on a user port is compared to the subnet of the VLAN for the user port; the packet is dropped if these two items do not match. Also applies to ARP packets.
bgp	Filters only BGP protocol packets from a TCP session that was not originated by the same switch that has this filter configured.
bpdu	Filters conventional Spanning Tree BPDU (destination MAC address 0x0180c2:000000) packets and GVRP (destination MAC address 0x0180c2:000021) packets.
rip	Filters RIP protocol packets.
ospf	Filters OSPF protocol packets.
vrrp	Filters VRRP protocol packets.
dvmrp	Filters IGMP packets with a type of 0x13. This applies only to IP packets with no options.
pim	Filters PIMv1, PIM-DM, and PIM-SM packets. The PIMv1 filter applies only to IP packets with no options.
isis	Filters IS-IS protocol packets.
dhcp-server	Filters response packets originating from a DHCP or BOOTP server that is configured on the known UDP port 67.
dns-reply	Filters all packets (both TCP and UDP) that originate from the known DNS port 53.

Defaults

parameter	default
filter	spooof
shutdown	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to disable the filter or shutdown function. This form of the command effects the overall operation of the feature.
- To specify more than one traffic type in the same command line, enter each type separated by a space (e.g., **spooof bgp ospf**).
- Note that existing traffic types to filter or shutdown are removed each time the **filter** or **shutdown** option is configured. Specify all desired traffic types each time the **qos user-port** command is performed to retain previously configured traffic types.
- No changes to the **filtering** and **shutdown** options are applied to the switch until the **qos apply** command is performed.
- This command only applies to ports that are members of the UserPorts group. Use the **policy port group** command to create and assign members to the UserPorts group.
- An SNMP trap is sent when a port is administratively disabled through a UserPorts shutdown function or a port disable action.
- To enable a port disabled by a user port shutdown operation, use the **interfaces admin** command to administratively enable the port or disconnect and reconnect the port cable.
- Up to 126 IP interfaces are supported with spooof 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 spooof bpdu
-> qos user-port shutdown spooof bgp ospf
-> qos no user-port shutdown
```

Release History

Release 7.1.1; command was 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 mapping and marking setting for all QoS ports. The DEI setting applies to packets marked yellow (non-conforming) as the result of Tri-Color Marking (TCM) rate limiting.

qos dei {ingress | egress}

qos no dei {ingress | egress}

Syntax Definitions

ingress	Maps the DEI/CFI bit to yellow (non-conforming) if this bit is set for ingress traffic.
egress	Marks the DEI/CFI bit for egress packets if TCM marked the packets yellow.

Defaults

By default, no DEI/CFI bit marking or mapping is done.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of this command to disable the global DEI bit mapping (ingress) or marking (egress) configuration for the switch.
- Use the **qos port dei** command to set the DEI bit mapping and marking configuration for a specific port. Note that the port setting takes precedence over the global DEI setting.
- Packets marked yellow by TCM rate limiting are still transmitted when there is no congestion on the egress port queues. Setting the DEI/CFI bit for yellow egress packets (**qos dei egress**) ensures that an upstream switch is made aware that the packet was marked yellow.
- When a switch receives a yellow packet with the DEI/CFI bit set and ingress DEI/CFI bit mapping is enabled (**qos dei ingress**), the packet is mapped to an internal drop precedence or yellow color marking for the switch.

Examples

```
-> qos dei ingress
-> qos dei egress
-> qos no dei ingress
-> qos no dei egress
```

Release History

Release 7.2.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos port dei	Configures the Drop Eligible Indicator (DEI) bit mapping and marking setting for the specified QoS port.
policy action cir	Configures a Tri-Color Marking policy action.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSConfigTable  
  alaQoSConfigDEIMapping  
  alaQoSConfigDEIMarking
```

debug qos

Configures the type of QoS events that will be displayed in the QoS log.

```
debug qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress]
```

```
debug no qos
```

```
debug no qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress]
```

Syntax Definitions

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. <i>Not supported for the OmniSwitch 6624/6648.</i>
port	Logs events related to QoS ports.
msg	Logs QoS messages.
classifier	Logs information whenever the switch classifies a flow; more details are provided if the log level is higher.
info	Logs basic information about the switch
config	Logs information about the global configuration.
main	Logs information about basic program interfaces.
sl	Logs information about source learning.
mem	Logs information about memory.
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.

Defaults

By default basic information messages are logged (**info**). Error messages are always logged.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to change the type of messages that will be logged or to return debugging to its default state.
- Use this command to troubleshoot QoS events on the switch.

Examples

```
-> debug qos flows queue
-> qos debug no flows no queue
-> debug no qos
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos forward log	Enables the switch to send events to the PolicyView application in real time.
qos log lines	Configures the number of lines in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable
  alaQoSConfigDebug
```

debug qos internal

Displays debugging information for QoS internal to the switch.

debug qos internal [*slice slot/slice*] [**flow**] [**queue**] [**port**] [**l2tree**] [**l3tree**] [**vector**] [**pending**] [**verbose**] [**mapper**] [**pool**] [**log**] [**pingonly** | **nopingonly**]

Syntax Definitions

<i>slot/slice</i>	The slot number and slice for which you want to view debugging information. A <i>slice</i> is a logical section of hardware that corresponds to particular ports on a network interface module.
flow	Displays information about QoS flows.
queue	Displays information about QoS queues.
port	Displays information about QoS ports.
l2tree	Displays information about Layer 2 flows.
l3tree	Displays information about Layer 3 flows.
vector	Displays information about vectors.
pending	Displays information about pending QoS objects.
verbose	Sets the output to verbose mode for more detailed information.
mapper	Displays information about QoS mapping flows to queues.
pool	Displays information about the buffer pool.
log	Displays information about QoS information that is logged.
pingonly	Specifies that any policies configured with an ICMP protocol condition apply only to ICMP echo-requests and echo-replies.
nopingonly	Configures the switch so that any policies configured with an ICMP protocol condition apply to any ICMP packets.

Defaults

Debugging is disabled by default.

parameter	default
pingonly nopingonly	nopingonly

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[debug qos](#)

Configures the type of QoS events that will be displayed in the QoS log.

clear qos log

Clears messages in the current QoS log.

```
clear qos log
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command is useful for clearing messages from a large log file so that the file is easier to view. Logs can get large if invalid rules are configured on the switch, or if a lot of QoS events have taken place. Clearing the log makes the file easier to manage.

Examples

```
-> clear qos log
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos log lines	Configures the number of lines in the QoS log.
debug qos	Configures the type of QoS events that will be displayed in the QoS log.
show qos log	Displays the log of QoS events.

MIB Objects

```
alaQoSConfigTable  
  alaQoSConfigClearLog
```

qos apply

Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).

qos apply

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is required to activate all QoS and policy commands. This is the only command that causes current changes to be written to flash.
- Rules are configured through the **policy rule** command, but are not active on the switch until you enter **qos apply**.

Examples

```
-> qos apply
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos revert	Removes any policies configured through policy rule but not applied to the current configuration through the qos apply command.
qos reset	Resets the QoS configuration to its default values.
qos flush	Deletes all pending policy information.

MIB Objects

```
alaQoSConfigTable  
  alaQoSConfigApply
```

qos revert

Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.

qos revert

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

policy rule	Configures a policy rule and saves it to the current configuration but does not make it active on the switch.
qos apply	Applies all QoS settings configured on the switch to the current configuration.
qos reset	Resets the QoS configuration to its defaults.

MIB Objects

```
alaQoSConfigTable  
  alaQoSConfigRevert
```

qos flush

Deletes all pending policy information. This command is different from **qos revert**, which returns the pending policy configuration to its last applied settings.

qos flush

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If you enter this command, the pending policy configuration is completely erased. If you then enter **qos apply**, the erased configuration *overwrites the applied policies and you will erase all of your policy configuration*.

Note. Do not use this command unless you want to erase all of your policy configuration and start configuring new policies.

- Use the **qos revert** command to return the pending policy configuration to its last applied value.
- Policy configuration includes the following commands:

base commands

policy rule	policy mac group
policy network group	policy port group
policy service	policy condition
policy service group	policy action

Examples

```
-> qos flush
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos revert

Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.

qos apply

Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).

policy server flush

Removes all cached LDAP policy data from the switch.

MIB Objects

alaQoSConfigTable
 alaQoSConfigFlush

qos reset

Resets the QoS configuration to its defaults.

```
qos reset
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[qos apply](#)

Applies all QoS settings configured on the switch to the current configuration.

[qos revert](#)

Deletes any QoS configuration that has not been applied to the configuration through the **qos apply** command.

MIB Objects

```
alaQoSConfigTable  
  alaQoSConfigReset
```

qos stats reset

Resets QoS statistic counters to zero.

```
qos stats reset
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use this command to reset global QoS statistics to zero. Statistics may be displayed with the **show qos statistics** command.

Examples

```
-> qos stats reset
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show qos statistics](#) Displays statistics about the QoS configuration.

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 10K, 6900

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 7.1.1; command was introduced.

MIB Objects

```
alaQoSPortTable  
  alaQoSPortSlot  
  alaQoSPortPort  
  alaQoSPortReset
```

qos port

Configures QoS parameters for a physical port. This section describes the base command with a single required option (*slot/port*).

In lieu of these options, the base command (**qos port**) may be used with other keywords to set up a QoS configuration on a per port basis. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

```
qos port slot/port[-port]  
    [trusted]  
    [maximum egress-bandwidth bps]  
    [maximum ingress-bandwidth bps]  
    [maximum depth bps]  
    [default 802.1p value]  
    [default dscp value]  
    [default classification {802.1p | tos | dscp}]
```

Syntax Definitions

slot/port[-*port*] The physical slot and port number. Use a hyphen to specify a range of ports (4/1-8).

Defaults

- All ports are untrusted.
- By default, QoS ports do not preempt queues of lower priority.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures whether the default mode for QoS ports is trusted or untrusted.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable
  alaQoSPortSlot
  alaQoSPortPort
  alaQoSPortTrusted
  alaQoSPortMaximumBandwidth
  alaQoSPortMaximumBandwidthStatus
  alaQoSPortMaximumIngBandwidth
  alaQoSPortMaximumIngBandwidthStatus
  alaQoSPortMaximumDefaultDepth
  alaQoSPortMaximumDefaultDepthStatus
  alaQoSPortDefault8021p
  alaQoSPortDefaultDSCP
  alaQoSPortDefaultClassification
```

qos port trusted

Configures whether an individual port is trusted or untrusted. Trusted ports can accept the 802.1p and ToS/DSCP values in incoming packets; untrusted ports will set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured.

qos port *slot/port*[-*port*] trusted

qos port *slot/port* no trusted

Syntax Definitions

slot/port[-*port*]

The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

Defaults

By default, all ports are untrusted.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **qos trust ports** command to set the default trust mode for all QoS ports. The **qos port trusted** command may be used to override the default.
- The setting applies only to ports with incoming traffic.
- Use the **qos port default 802.1p** or **qos port default dscp** commands to specify that a value other than zero should be applied to the incoming packets. Note that this value is overridden if a policy exists that specifies a different 802.1p or ToS/DSCP value for such packets.

Examples

```
-> qos port 3/1 trusted
-> qos port 4/2 no trusted
```

Release History

Release 7.1.1; command was introduced.

Related Commands**qos apply**

Applies configured QoS and policy settings to the current configuration.

qos port

Configures a physical port for QoS.

qos trust ports

Configures the global trust mode for QoS ports.

show qos port

Displays information about QoS ports.

MIB Objects

alaQoSPortTable

 alaQoSPortTrusted

qos port maximum egress-bandwidth

Configures the maximum rate at which to send traffic on the specified QoS port.

qos port *slot/port[-port]* **maximum egress-bandwidth** *bps[k | m | g | t]*

qos port *slot/port[-port]* **no maximum egress-bandwidth**

Syntax Definitions

slot/port[-port] The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

bps[k | m | g | t] The maximum amount of bandwidth, in bits-per-second, for all traffic that egresses on the port. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k**, **5m**, **1g**, **1t**).

Defaults

By default, the maximum bandwidth is the maximum allowed for the interface type on which the port resides.

parameter	default
<i>k m g t</i>	k

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a configured maximum egress bandwidth value from a port.
- If the maximum egress bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number **10** is specified, **10K** is the maximum bandwidth value used. However, if **10G** is specified, the maximum bandwidth value applied is **10** gbps.
- 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 4/1-8 maximum egress-bandwidth 10m
-> qos port 3/1 no maximum egress-bandwidth
-> qos port 4/1-8 no maximum egress-bandwidth
```

Release History

Release 7.1.1; command was 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[-port]* **maximum ingress-bandwidth** *bps[k | m | g | t]*

qos port *slot/port[-port]* **no maximum ingress-bandwidth**

Syntax Definitions

slot/port[-port] The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

bps[k | m | g | t] The maximum amount of bandwidth, in bits-per-second, for all traffic that ingresses on the port. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k**, **5m**, **1g**, **1t**).

Defaults

By default, the maximum bandwidth is the maximum allowed for the interface type on which the port resides.

parameter	default
<i>k m g t</i>	k

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a configured maximum ingress bandwidth value from a port.
- If the maximum ingress bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number **10** is specified, **10K** is the maximum bandwidth value used. However, if **10G** is specified, the maximum bandwidth value applied is **10** gbps.
- 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 4/1-8 maximum ingress-bandwidth 10m
-> qos port 3/1 no maximum ingress-bandwidth
-> qos port 4/1-8 no maximum ingress-bandwidth
```

Release History

Release 7.1.1; 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 maximum depth

Configures the maximum bucket size used for traffic metering. The bucket size determines how much the traffic can burst over the maximum bandwidth rate.

qos port *slot/port[-port]* **maximum depth** *bps[k | m | g | t]*

qos port *slot/port[-port]* **no maximum depth**

Syntax Definitions

slot/port[-port] The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

bps[k | m | g | t] The maximum bucket size, in bits-per-second. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k**, **5m**, **1g**).

Defaults

parameter	default
<i>k m g t</i>	k

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This QoS port parameter is configured in conjunction with the maximum bandwidth parameters. When the bucket size is reached, the switch starts to drop packets.
- Use the **no** form of the command to remove the maximum depth setting from a port.
- If the maximum depth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number **10** is specified, **10K** is the maximum depth value used. However, if **10G** is specified, the maximum depth value applied is **10** gbps.
- Modifying the maximum depth is most useful for low-bandwidth links.

Examples

```
-> qos port 3/1 maximum depth 100
-> qos port 4/1-8 maximum depth 10m
-> qos port 3/1 no maximum depth
-> qos port 4/1-8 no maximum depth
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable  
  alaQoSPortSlot  
  alaQoSPortPort  
  alaQoSPortMaximumDefaultDepth
```

qos port default 802.1p

Configures the 802.1p value to be inserted in flows ingressing on an untrusted port.

qos port *slot/port*[-*port*] **default 802.1p** *value*

Syntax Definitions

<i>slot/port</i> [- <i>port</i>]	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
<i>value</i>	The priority value to be set. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- By default untrusted ports will set the 802.1p bit to zero on incoming flows. Use this command to specify that a different 802.1p value should be applied to the flow.
- The default 802.1p value is not used if there is a matching QoS policy rule that sets the priority.
- Note that 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
-> qos port 4/1-8 default 802.1p 7
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

alaQoSPortTable
 alaQoSPortDefault8021p

qos port default dscp

Configures the ToS/DSCP value to be inserted in flows ingressing on an untrusted port.

```
qos port slot/port[-port] default dscp value
```

Syntax Definitions

slot/port[-port] The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

value The ToS/DSCP value. The range is 0–63.

Defaults

parameter	default
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The value configured by this command sets the upper byte (precedence) and therefore configures the ToS/DSCP value for the port.
- The default DSCP value is not used if there is a matching QoS policy rule that sets the priority.
- Note that on the 802.1p bit for tagged packets received on untrusted ports is set with the default 802.1p value, which is configured using the [qos port default 802.1p](#) command. If the packet is untagged, however, then the DSCP bit is set with the default DSCP value, which is configured using the [qos port default dscp](#) command.

Examples

```
-> qos port 3/1 default dscp 63  
-> qos port 4/1-8 default dscp 33
```

Release History

Release 7.1.1; command was introduced.

Related Commands**qos apply**

Applies configured QoS and policy settings to the current configuration.

qos port

Configures a physical port for QoS.

show qos port

Displays information about QoS ports.

MIB Objects

alaQoSPortTable

alaQoSPortDefaultDSCP

qos port default classification

Specifies the default egress priority value to use for IP traffic ingressing on trusted ports.

qos port *slot/port[-port]* **default classification** {**tos** | **802.1p** | **dscp**}

Syntax Definitions

<i>slot/port[-port]</i>	The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
tos	Specifies that the ToS value of the flow will be used to prioritize flows coming in on the port.
802.1p	Specifies that the 802.1p value of the flow will be used to prioritize flows coming in on the port.
dscp	Specifies that the DSCP value of the flow will be used to prioritize flows coming in on the port.

Defaults

parameter	default
tos 802.1p dscp	dscp

Platforms Supported

OmniSwitch 10K, 6900

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 may be dropped before any QoS rules can take effect for the traffic.

Examples

```
-> qos port 8/24 default classification dscp
-> qos port 4/1-8 default classification dscp
-> qos port 7/1 default classification 802.1p
-> qos port 5/1-8 default classification 802.1p
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
qos port	Configures a physical port for QoS.
show qos port	Displays information about QoS ports.

MIB Objects

alaQoSPortTable
alaQoSPortDefaultClassification

qos port dei

Configures the Drop Eligible Indicator (DEI) bit mapping and marking setting for the specified QoS port. The DEI setting applies to packets marked yellow (non-conforming) as the result of Tri-Color Marking (TCM) rate limiting.

```
qos port slot/port dei {ingress | egress}
```

```
qos port slot/port no dei {ingress | egress}
```

Syntax Definitions

<i>slot/port</i>	The slot number and port number of the physical port.
ingress	Maps the DEI/CFI bit to yellow (non-conforming) if this bit is set for ingress packets.
egress	Sets the DEI/CFI bit for egress packets if TCM marked the packets yellow.

Defaults

By default, no DEI/CFI bit mapping or marking is done.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of this command to disable the DEI bit mapping (ingress) or marking (egress) configuration for the specified port
- Use the **qos dei** command to set the global DEI bit mapping and marking configuration for all QoS switch ports. Note that the port-level setting takes precedence over the global DEI setting.
- Packets marked yellow by TCM rate limiting are still transmitted when there is no congestion on the egress port queues. Setting the DEI/CFI bit for yellow egress packets (**qos port dei egress**) ensures that an upstream switch is made aware that the packet was marked yellow.
- When a switch receives a yellow packet with the DEI/CFI bit set and ingress DEI/CFI bit mapping is enabled (**qos port dei ingress**), the packet is mapped to an internal drop precedence or yellow color marking for the switch.

Examples

```
-> qos port 1/10 dei ingress
-> qos port 1/20 dei egress
-> qos port 1/10 no dei ingress
-> qos port 1/20 no dei egress
```

Release History

Release 7.2.1; command was introduced.

Related Commands

qos port	Configures a physical port for QoS.
qos dei	Configures the global Drop Eligible Indicator (DEI) bit mapping and marking setting for all QoS ports.
policy action cir	Configures a Tri-Color Marking policy action.
show qos config	Displays global information about the QoS configuration.
show qos port	Displays information about QoS ports.

MIB Objects

```
alaQoSPortTable  
  alaQoSPortDEIMapping  
  alaQoSPortDEIMarking
```

qos qsi qsp

Configures the QSet profile (QSP) association for the specified QSet instance (QSI). A QSI is a set of eight queues that is automatically associated with each port and link aggregate (LAG) ID.

```
qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} qsp {qsp_id | qsp_name}
```

Syntax Definitions

<i>slot/port[-port]</i>	The physical slot and port number to associate with the QSet. Use a hyphen to specify a range of ports (3/1-10).
<i>slot</i>	The slot number to associate with the QSet.
<i>agg_id[-agg_id]</i>	The link aggregate ID to associate with the QSet. Use a hyphen to specify a range of IDs (10-20).
<i>qsp_id</i>	An existing QSet profile (QSP) ID number to assign to this instance. The valid range is 1–4.
<i>qsp_name</i>	An existing QSet profile name (qsp-1, qsp-2, qsp-3, qsp-4) to assign to this instance.

Defaults

By default, QSP 1 is assigned to each QSet instance.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- There is only one QSI per port or LAG ID and only one QSP associated with the QSI.
- A QSI hierarchy exists consisting of parent/child relationships. For example, all member ports of a link aggregate will import the QSI/QSP settings of the parent link aggregate. When a member port moves out of the link aggregate, the QSI/QSP settings for that port are reset to the default settings.
- The number of children supported for a LAG ID is 8.

Examples

```
-> qos qsi port 1/2 qsp 2
-> qos qsi port 2/1-10 qsp 3
-> qos qsi slot 3 qsp 4
-> qos qsi linkagg 10 qsp 2
```

Release History

Release 7.2.1.R02; command introduced.

Related Commands

<code>qos qsi wred</code>	Configures the WRED administrative status for a QSet instance.
<code>qos qsi stats</code>	Configures statistics collection for the QSet instance.
<code>show qos qsi</code>	Displays the QSet instance configuration.
<code>show qos qsp</code>	Displays the QSet profile attributes.

MIB Objects

```
alcatelIND1VfcMIB  
alaVfcQsetInstanceTable  
  alaVfcQsetQSPId  
  alaVfcQsetQSPName  
  alaVfcQsetWRPAdminState  
  alaVfcQsetStatsAdmin  
  alaVfcQsetStatsInterval
```

qos qsi wred

Configures the WRED profile (WRP) administrative status for the QSet profile associated with the specified QSet instance (QSI). A QSI is a set of eight queues that is automatically associated with each port and link aggregate (LAG) ID.

```
qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} wred admin-state {enable | disable}
```

Syntax Definitions

<i>slot/port[-port]</i>	The physical slot and port number to associate with the QSet. Use a hyphen to specify a range of ports (3/1-10).
<i>slot</i>	The slot number to associate with the QSet.
<i>agg_id[-agg_id]</i>	The link aggregate ID to associate with the QSet. Use a hyphen to specify a range of IDs (10-20).
wred admin-state enable	Enables the WRED profile for the instance.
wred admin-state disable	Disables the WRED profile for the instance.

Defaults

By default, WRED is disabled for the QSet instance.

Platforms Supported

OmniSwitch 6900
OmniSwitch 10K; WRED is not supported.

Usage Guidelines

- There is only one QSI per port or LAG ID and only one profile (WRP 1) associated with the QSI.
- Changing the WRED profile status for a QSI only changes the status for the port or link aggregate to which the QSI is associated.
- WRP 1 is the only profile supported. Configuring additional profiles is not supported at this time.
- When enabled, WRP 1 applies the following color threshold values only to TCP traffic. The threshold values indicated are a percentage of the maximum average queue length.

Color	Min Threshold	Max Threshold	Drop Probability	Gain
Red	10	50	36	9
Yellow	50	90	30	9
Green	90	100	24	9

Examples

```
-> qos qsi port 1/2 wred admin-state enable
-> qos qsi port 2/1-10 wred admin-state disable
```

```
-> qos qsi slot 3 wred admin-state enable
-> qos qsi linkagg 10 wred admin-state enable
```

Release History

Release 7.2.1.R02; command introduced.

Related Commands

qos qsi qsp	Configures the QSet profile association for the QSet instance.
qos qsi stats	Configures statistics collection for the QSet instance.
show qos qsi	Displays the QSet instance configuration..

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsetInstanceTable
  alaVfcQsetQSPID
  alaVfcQsetQSPName
  alaVfcQsetWRPAdminState
  alaVfcQsetStatsAdmin
  alaVfcQsetStatsInterval
```

qos qsi stats

Configures the statistics collection administrative status and interval for the specified QSet instance (QSI). A QSI is a set of eight queues that is automatically associated with each port and link aggregate (LAG) ID.

```
qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} stats {admin-state {enable | disable} | interval interval_time}}
```

Syntax Definitions

<i>slot/port</i> [- <i>port</i>]	The physical slot and port number to associate with the QSet. Use a hyphen to specify a range of ports (3/1-10).
<i>slot</i>	The slot number to associate with the QSet.
<i>agg_id</i> [- <i>agg_id</i>]	The link aggregate ID to associate with the QSet. Use a hyphen to specify a range of IDs (10-20).
stats admin-state enable	Enables statistics collection for the instance.
stats admin-state disable	Disables statistics collection for the instance.
<i>interval_time</i>	The time interval for statistics gathering. The valid range is 10 to 300 seconds.

Defaults

By default, statistics collection is disabled and the time interval is set to 10 seconds.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- There is only one QSI per port or LAG ID and only one Qset profile (QSP) or DCB profile (DCP) associated with the QSI.
- Changing the statistics collection status for a QSI only changes the status for the port or link aggregate to which the QSI is associated.

Examples

```
-> qos qsi port 1/2 stats admin-state enable
-> qos qsi port 1/2 stats interval 30
-> qos qsi port 2/1-10 stats admin-state enable
-> qos qsi slot 3 stats admin-state enable interval 250
-> qos qsi linkagg 10 stats admin-state enable interval 120
```

Release History

Release 7.2.1.R02; command introduced.

Related Commands

qos qsi qsp	Configures the QSet profile association for the QSet instance.
qos qsi wred	Configures the WRED administrative status for the QSet instance.
show qos qsi	Displays the QSet instance configuration.
show qos qsi stats	Displays statistics for one or more QSet instances.

MIB Objects

```
alcatelIND1VfcMIB  
alaVfcQsetInstanceTable  
  alaVfcQsetQSPID  
  alaVfcQsetQSPName  
  alaVfcQsetWRPAdminState  
  alaVfcQsetStatsAdmin  
  alaVfcQsetStatsInterval
```

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 10K, 6900

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   Bandwidth   DEI
Port  Active Trust P/DSCP Classification  Physical Ingress Egress  Map/Mark  Type
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
1/1     No      No  0/ 0          DSCP          0K           -      -      No / No  ethernet
1/2     Yes     No  0/ 0          DSCP          1.00G        -      -      No / No  ethernet-1G
1/3     No      No  0/ 0          DSCP          0K           -      -      No / No  ethernet
1/4     No      No  0/ 0          DSCP          0K           -      -      No / No  ethernet
1/5     No      No  0/ 0          DSCP          0K           -      -      No / No  ethernet
1/6     No      No  0/ 0          DSCP          0K           -      -      No / No  ethernet
1/7     No      No  0/ 0          DSCP          0K           -      -      No / No  ethernet
1/8     No      No  0/ 0          DSCP          0K           -      -      No / No  ethernet
1/9     No      No  0/ 0          DSCP          0K           -      -      No / No  ethernet
1/10    No      No  0/ 0          DSCP          0K          50K      -      No / No  ethernet
1/11    No      *Yes 0/ 0          *802.1P       0K           -      -      No / No  ethernet
1/12    No      *Yes 0/ 0          *802.1P       0K           -      -      No / No  ethernet
```



```

-> show qos port 1/2
Slot/          Default      Default      Bandwidth      DEI
Port  Active Trust P/DSCP Classification  Physical Ingress Egress  Map/Mark      Type
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
1/2   Yes   No  0/ 0          DSCP          1.00G      -      -   No / No   ethernet-1G

```

output definitions

Slot/Port	The slot and physical port number.
Active	Whether or not the port is sending/receiving QoS traffic.
Trust	Whether the port is trusted or not trusted. Configured through the qos port trusted command.
Default P	The default 802.1p setting for the port. Configured through the qos port default 802.1p command.
Default DSCP	The default ToS/DSCP setting for the port. Configured through the qos port default dscp command.
Default Classification	The default classification setting for the port (802.1p , ToS , or DSCP). Configured through the qos port default classification command.
Physical Bandwidth	The amount of physical bandwidth available on the port.
Ingress Bandwidth	The amount of ingress bandwidth configured for the port. Configured through the qos port maximum ingress-bandwidth command.
Egress Bandwidth	The amount of egress bandwidth configured for the port. Configured through the qos port maximum egress-bandwidth command.
DEI Map/Mark	The Drop Eligible Indicator (DEI) bit mapping and marking setting for the port. Configured through the qos port dei command.
Type	The interface type, ethernet or wan .

Release History

Release 7.1.1; command was introduced.

Related Commands

qos port Configures a physical port for QoS.

MIB Objects

```

alcatelIND1VfcMIB
alaQoSPortTable
  alaQoSPortSlot
  alaQoSPortPort
  alaQoSPortEnabled
  alaQoSPortDefault8021p
  alaQoSPortDefaultDSCP
  alaQoSPortMaximumDefaultBandwidth
  alaQoSPortDefaultClassification

```

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 10K, 6900

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  Triumph2   16/16      0  128/101     128/101     64/64
        1      128/125     1  128/125     128/125     64/64
        2      128/0       2  128/0       128/0       64/64
        3      128/0       3  128/0       128/0       64/64
        4      128/0       4  128/0       128/0       64/64
        5      128/0       5  128/0       128/0       64/64
        6      128/0       6  128/0       128/0       64/64
        7      128/0       7  128/0       128/0       64/64
        8      128/0       8  128/0       128/0       64/64
        9      128/0      10  128/0       128/0       64/64
       10     128/0      11  128/0       128/0       64/64
       11     128/0      12  128/0       128/0       64/64
       12     128/0      13  128/0       128/24      64/64
       13     128/0      14  128/0       128/62      64/64
       14     128/0      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 7.1.1; command was introduced.

Related Commands

[policy rule](#) Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

N/A

show qos log

Displays the log of QoS events.

show qos log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use this command to display the current QoS log. To clear the log, use the **qos clear log** command.

Examples

```
-> show qos log
**QOS Log**
Insert rule 0
Rule index at 0
Insert rule 1
Rule index at 1
Insert rule 2
Rule index at 2
Enable rule r1 (1) 1,1
Enable rule r2 (0) 1,1
Enable rule yuba1 (2) 1,1
Verify rule r1(1)
Enable rule r1 (1) 1,1
Really enable r1
Update condition c1 for rule 1 (1)
Verify rule r2(1)
Enable rule r2 (0) 1,1
Really enable r2
Update condition c2 for rule 0 (1)
Verify rule yuba1(1)
Enable rule yuba1 (2) 1,1
Really enable yuba1
Update condition yubamac for rule 2 (1)
QoS Manager started TUE MAR 10 13:46:50 2002

Match rule 2 to 1
Match rule 2 to 2
Match rule 2 to 3
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[qos clear log](#)

Clears messages in the current QoS log.

[qos log lines](#)

Configures the number of lines in the QoS log.

MIB Objects

N/A

show qos config

Displays global information about the QoS configuration.

show qos config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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,
  Admin                               = enable,
  Trust ports                          = no,
  Phones                               = trusted,
  Log lines                            = 10240,
  Log level                             = 5,
  Log console                          = no,
  Forward log                          = no,
  Stats interval                       = 5,
  User-port filter                     = spoof,
  User-port shutdown                  = none,
  Debug                               = info,
  Pending changes                     = port
```

output definitions

Admin	Whether or not QoS is enabled or disabled. Configured through the qos command.
Trust Ports	The default trusted mode for switch ports. Configured through the qos trust ports command.
Phones	Whether or not IP Phone traffic is automatically trusted or assigned a priority value. Configured through the qos phones command.
Log lines	The number of lines included in the QoS log. Configured through the qos log lines command.
Log level	The level of log detail. Configured through the qos log level command.

output definitions (continued)

Log console	Whether or not log messages are sent to the console. Configured through the qos log console command.
Forward log	Whether or not logged events are sent to the policy server software in the switch in real time. Configured through the qos forward log command.
Stats interval	How often the switch polls network interfaces for statistics about QoS events. Configured through the qos stats interval command.
User-port filter	The type of traffic that is filtered on ports that are members of the UserPorts group. Configured through the qos user-port command.
User-port shutdown	The type of traffic that will trigger an administrative shutdown of the port if the port is a member of the UserPorts group. Configured through the qos user-port command.
Debug	The type of information that will be displayed in the QoS log. A value of info indicates the default debugging type.
Pending changes	QoS changes not yet applied to the configuration.

Release History

Release 7.1.1; command was introduced.

Related Commands

qos	Enables or disables QoS. This base command may be used with key-word options to configure QoS globally on the switch.
show qos statistics	Displays statistics about the QoS configuration.

MIB Objects

```

alaQoSConfigTable
  alaQoSConfigEnable
  alaQoSConfigTrustPorts
  alaQoSConfigAutoPhones
  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 10K, 6900

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		

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.

output definitions (continued)

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.

Release History

Release 7.1.1; command was introduced.

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

show qos wrp

Displays the Weighted Random Early Detection (WRED) profile (WRP) configuration for the switch.

show qos wrp [*wrp_id* | *wrp_name*] [**detail** [**port** *slot/port*[-*port*]] | **slot** *slot* | **linkagg** *agg_id*[-*agg_id*]]

Syntax Definitions

<i>wrp_id</i>	A WRED profile (WRP) ID number. The valid range is 1.
<i>wrp_name</i>	A WRED profile name.
detail	Displays WRED profile configuration details for a port, slot, or link aggregate.
<i>slot/port</i> [- <i>port</i>]	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>slot</i>	A slot number. Displays information for all ports on the slot.
<i>agg_id</i> [- <i>agg_id</i>]	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the *wrp_id* or the *wrp_name* parameter to display information for a specific profile.
- Use the **detail** parameter to display additional profile information, such as the profile configuration associated with queues and ports.
- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to display profile information associated with specific ports or link aggregates. These parameters are used in combination with the **detail** parameter.

Examples

```
-> show qos wrp
WRP 1 (wrp-1)
  #Ports: 480, MTU: 1540
  Red
    Min-Th: 10, Max-Th: 50, Max-Pb: 36, Gain: 9
  Yellow
    Min-Th: 50, Max-Th: 90, Max-Pb: 30, Gain: 9
  Green
    Min-Th: 90, Max-Th: 100, Max-Pb: 24, Gain: 9
```

output definitions

WRP	The WRED profile (WRP) ID number and name.
#Ports	The number of ports to which this profile is attached.
MTU	The MTU size.
Min-Th	The minimum queue threshold percentage for red, green, and yellow packets.
Max-Th	The maximum queue threshold percentage for red, green, and yellow packets.
Max-Pb	The maximum drop probability percentage for red, green, and yellow packets.
Gain	The gain value to smooth out the queue (1–15).

```
-> show qos wrp 1 detail port 2/4
```

```
Port 2/4
```

```

QSAP:   Port 2/4, Parent:   Port 2/4,
WRP:   1, Name:             wrp-1, Admin: Dis
  QSI   Port 2/4
    QSP: 1, Name:           qsp-1, Admin: Ena
      QI 1
        WRP: 1, Name:       wrp-1, Admin: Dis
      QI 2
        WRP: 1, Name:       wrp-1, Admin: Dis
      QI 3
        WRP: 1, Name:       wrp-1, Admin: Dis
      QI 4
        WRP: 1, Name:       wrp-1, Admin: Dis
      QI 5
        WRP: 1, Name:       wrp-1, Admin: Dis
      QI 6
        WRP: 1, Name:       wrp-1, Admin: Dis
      QI 7
        WRP: 1, Name:       wrp-1, Admin: Dis
      QI 8
        WRP: 1, Name:       wrp-1, Admin: Dis

```

output definitions

Port	The physical slot and port number (or link aggregate ID for a logical port).
QSAP	The QSet attachment point (QSAP). This is a logical entity used internally by the switch to identify the association between a QSet instance and a port or link aggregate. The QSAP is not configurable at this time.
Parent	The QSAP ID for the parent QSAP, if any.
WRP Name Admin	The WRED profile (WRP) ID number, name, and administrative status.
QSI	The switch port associated with the QSet instance (QSI).
QSP Name Admin	The QSet profile (QSP) ID number, name, and administrative status.
QI 1..8	The WRP information for each of the QSet queues.

Release History

Release 7.2.1; command was introduced.

Related Commands

qos qsi wred	Configures the administrative status of the WRED profile.
qos qsi qsp	Changes the QSet profile association for a QSet instance.
show qos qsi	Displays the QSet instance configuration.

MIB Objects

```
alcatelIND1VfcMIB  
alaVfcWREDProfileTable  
  alaVfcWRPId  
  alaVfcWRPAdminState  
  alaVfcWRPName  
  alaVfcWRPGreenMinThreshold  
  alaVfcWRPGreenMaxThreshold  
  alaVfcWRPGreenMaxDropProbability  
  alaVfcWRPGreenGain  
  alaVfcWRPYellowMinThreshold  
  alaVfcWRPYellowMaxThreshold  
  alaVfcWRPYellowMaxDropProbability  
  alaVfcWRPYellowGain  
  alaVfcWRPRedMinThreshold  
  alaVfcWRPRedMaxThreshold  
  alaVfcWRPRedMaxDropProbability  
  alaVfcWRPRedGain  
  alaVfcWRPMTU  
  alaVfcWRPAttachmentCount  
  alaVfcWRPLastChange  
  alaVfcWRPRowStatus
```

show qos qsp

Displays the QSet profile (QSP) configuration for the switch.

```
show qos qsp [qsp_id | qsp_name] [detail [port slot/port[-port]] | slot slot | linkagg agg_id[-agg_id]]
```

Syntax Definitions

<i>qsp_id</i>	A QSet profile (QSP) ID number. The valid range is 1–4.
<i>qsp_name</i>	A QSP profile name.
detail	Displays QSP configuration details for a specific profile, port, slot, or link aggregate.
<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>slot</i>	A slot number. Displays information for all ports on the slot.
<i>agg_id[-agg_id]</i>	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

By default, displays the configuration for all four of the QSet profiles (QSP 1–4).

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the *qse_id* or the *qsp_name* parameter to display information for a specific profile.
- Use the **detail** parameter to display additional profile information for all ports and link aggregates.
- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to display profile information associated with specific ports or link aggregates. These parameters are used in combination with the **detail** parameter.

Examples

```
-> show qos qsp 2
QSP 2 (qsp-2)
#Ports:    0, #Queues:  8, BW (%): 100,
WRP:  1, Name:      wrp-1,
Scheduler: Qspec, Type: Default
Template: 2, Name:   qsp-2
  QP 1
    Qtype:  EF,
    WRP:  1, Name:      wrp-1,
    CIR (%):  0, PIR (%):  20
    WFQ-Mode: WERR, WFQ-Weight:  1
  QP 2
    Qtype:  SP7,
    WRP:  1, Name:      wrp-1,
```

```

    CIR (%): 0, PIR (%): 100
    WFQ-Mode: WERR, WFQ-Weight: 1
QP 3
    Qtype: SP5,
    WRP: 1, Name: wrp-1,
    CIR (%): 0, PIR (%): 100
    WFQ-Mode: WERR, WFQ-Weight: 1
QP 4
    Qtype: SP4,
    WRP: 1, Name: wrp-1,
    CIR (%): 0, PIR (%): 100
    WFQ-Mode: WERR, WFQ-Weight: 1
QP 5
    Qtype: SP3,
    WRP: 1, Name: wrp-1,
    CIR (%): 0, PIR (%): 100
    WFQ-Mode: WERR, WFQ-Weight: 1
QP 6
    Qtype: SP2,
    WRP: 1, Name: wrp-1,
    CIR (%): 0, PIR (%): 100
    WFQ-Mode: WERR, WFQ-Weight: 1
QP 7
    Qtype: SP1,
    WRP: 1, Name: wrp-1,
    CIR (%): 0, PIR (%): 100
    WFQ-Mode: WERR, WFQ-Weight: 1
QP 8
    Qtype: SP0,
    WRP: 1, Name: wrp-1,
    CIR (%): 0, PIR (%): 100
    WFQ-Mode: WERR, WFQ-Weight: 1

```

output definitions

QSP	The QSet profile (QSP) ID number and name.
#Ports	The number of ports to which this profile is attached.
#Queues	The number of queues associated with this QSet. Currently there are eight queues for each QSet.
BW%	The bandwidth percentage for the QSet. The bandwidth is shared between all the queues.
WRP	The WRED profile (WRP) ID number associated with the QSet.
Name	The WRP name.
Scheduler	The type of scheduler, such as queue specific priority (Qspec) or strict priority.
Type	Whether the QSP is static or dynamic. Currently there are 4 pre-defined, static profiles (QSP 1–4). User-configured, dynamic profiles are not supported at this time.
QP 1...8	The queue profile configuration for each QSet queue. The configuration for each of the individual queue profiles is defined by the QSP in use. For example, QSP 1 applies a different queue configuration than QSP 2, 3, or 4.

```
-> show qos qsp 1 detail
```

```
Legends: T (Type): D = Default, C = Custom
```

QSAP Port	QSAP Type	dQSI	ID	Name	QSAP Parent	Admin	Oper	BW (%) Admin	BW (Mbps) Oper	T
1/1	Phy	Port 1/1	1	qsp-1	Port 1/1	Ena	Dis	100	0	D
1/2	Phy	Port 1/2	1	qsp-1	Port 1/2	Ena	Dis	100	0	D
1/3	Phy	Port 1/3	1	qsp-1	Port 1/3	Ena	Dis	100	0	D
1/4	Phy	Port 1/4	1	qsp-1	Port 1/4	Ena	Dis	100	0	D
1/5	Phy	Port 1/5	1	qsp-1	Port 1/5	Ena	Dis	100	0	D
.										
2/1	Phy	Port 2/1	1	qsp-1	Port 2/1	Ena	Dis	100	0	D
2/2	Phy	Port 2/2	1	qsp-1	Port 2/2	Ena	Ena	100	0	D
2/3	Phy	Port 2/3	1	qsp-1	Port 2/3	Ena	Dis	100	0	D
2/4	Phy	Port 2/4	1	qsp-1	Port 2/4	Ena	Dis	100	0	D
10	Log	Linkagg 10	1	qsp-1	Linkagg 10	Ena	Ena	100	0	D

```
-> show qos qsp 1 detail port 1/4
```

```
Legends: T (Type): D = Default, C = Custom
```

QSAP Port	QSAP Type	dQSI	ID	Name	QSAP Parent	Admin	Oper	BW (%) Admin	BW (Mbps) Oper	T
1/4	Phy	Port 1/4	1	qsp-1	Port 1/4	Ena	Dis	100	0	D

output definitions

QSAP Port	The port number or link aggregate ID for the QSet attachment point (QSAP). A QSAP is a logical entity generated internally by the switch to identify the association between a QSet instance and a port or link aggregate. The QSAP is not configurable at this time.
QSAP Type	The type of QSAP port; Phy = physical (slot/port), Log = logical (link-aggregate ID).
dQSI	The default QSet instance (dQSI) ID number. This number is generated internally by the switch to identify the QSI that is automatically assigned to each port and link aggregate.
ID	The QSet profile (QSP) ID number.
Name	The QSP name.
QSAP Parent	The QSAP parent ID number.
Admin	The administrative state of the QSet.
Oper	The operational state of the QSet.
BW (%) Admin	The administrative bandwidth percentage for the QSet. The administrative percentage is not configurable at this time.
BW (Mbps)Oper	The operational bandwidth value, which is based on port speed.
Type	Whether the QSet profile is a default profile (D = default templates 1–4) or a custom profile (C = user-configured 5–8). Configuring a custom profile is not supported at this time.

Release History

Release 7.2.1; command was introduced.

Related Commands

qos qsi qsp	Changes the QSet profile association for a QSet instance.
qos qsi wred	Configures the administrative status of the WRED profile.
show qos qsi	Displays the QSet instance configuration.

MIB Objects

```
alcatelIND1VfcMIB  
alaVfcQsetProfileTable  
  alaVfcQSPId  
  alaVfcQSPName  
  alaVfcQSPBandwidthLimitValue  
  alaVfcQSPQueueCount  
  alaVfcQSPWRPId  
  alaVfcQSPWRPAdminState  
  alaVfcQSPSchedulingMethod  
  alaVfcQSPStatsAdmin  
  alaVfcQSPAttachmentCount
```

show qos qsi

Displays the QSet instance (QSI) configuration for the switch. A QSI is a logical set of eight virtual output queues (OmniSwitch 10K) or eight egress queues (OmniSwitch 6900) associated with each port and link aggregate (LAG) ID.

show qos qsi [**port** *slot/port*[-*port*] | **slot** *slot* | **linkagg** *agg_id*[-*agg_id*]] [**detail**]

Syntax Definitions

<i>slot/port</i> [- <i>port</i>]	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>slot</i>	A slot number. Displays information for all ports on the slot.
<i>agg_id</i> [- <i>agg_id</i>]	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
detail	Displays additional queue information for the instance.

Defaults

By default, displays the entire QSI configuration for the switch.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to display the QSI information associated with specific ports or link aggregates.
- Use the **detail** parameter to display additional profile information, such as the profile configuration associated with queues and ports.

Examples

```
-> show qos qsi port 1/1
Port 1/1
  QSAP:    Port 1/1, Parent:    Port 1/1
  QSI     Port 1/1
    QSP:   1, Name:             qsp-1, Admin: Ena, Oper: Dis,
    WRP:   1, Name:             wrp-1, Admin: Dis, Oper: Dis,
    Stats
      Admin: Dis, Oper: Dis, Interval:    10
    BW
      Admin (%): 100, Oper (Mbps):       0

-> show qos qsi port 1/1 detail
Port 1/1
  QSAP:    Port 1/1, Parent:    Port 1/1
  QSI     Port 1/1
    QSP:   1, Name:             qsp-1, Admin: Ena, Oper: Dis,
    WRP:   1, Name:             wrp-1, Admin: Dis, Oper: Dis,
    Stats
```

```
Admin: Dis, Oper: Dis, Interval: 10
BW
Admin (%): 100, Oper (Mbps): 0
QI 1
Admin: Ena, Oper: Dis, Qtype: SP7,
WRP: 1, Name: wrp-1, Admin: Dis, Oper: Dis,
Stats
Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (Mbps): 0
PIR
Admin (%): 100, Oper (Mbps): 0
QI 2
Admin: Ena, Oper: Dis, Qtype: SP6,
WRP: 1, Name: wrp-1, Admin: Dis, Oper: Dis,
Stats
Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (Mbps): 0
PIR
Admin (%): 100, Oper (Mbps): 0
QI 3
Admin: Ena, Oper: Dis, Qtype: SP5,
WRP: 1, Name: wrp-1, Admin: Dis, Oper: Dis,
Stats
Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (Mbps): 0
PIR
Admin (%): 100, Oper (Mbps): 0
QI 4
Admin: Ena, Oper: Dis, Qtype: SP4,
WRP: 1, Name: wrp-1, Admin: Dis, Oper: Dis,
Stats
Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (Mbps): 0
PIR
Admin (%): 100, Oper (Mbps): 0
QI 5
Admin: Ena, Oper: Dis, Qtype: SP3,
WRP: 1, Name: wrp-1, Admin: Dis, Oper: Dis,
Stats
Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (Mbps): 0
PIR
Admin (%): 100, Oper (Mbps): 0
QI 6
Admin: Ena, Oper: Dis, Qtype: SP2,
WRP: 1, Name: wrp-1, Admin: Dis, Oper: Dis,
Stats
Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (Mbps): 0
PIR
Admin (%): 100, Oper (Mbps): 0
QI 7
Admin: Ena, Oper: Dis, Qtype: SP1,
```

```

WRP: 1, Name:          wrp-1, Admin: Dis, Oper: Dis,
  Stats
    Admin: Dis, Oper: Dis
  CIR
    Admin (%): 0, Oper (Mbps): 0
  PIR
    Admin (%): 100, Oper (Mbps): 0
QI 8
Admin: Ena, Oper: Dis, Qtype: SP0,
WRP: 1, Name:          wrp-1, Admin: Dis, Oper: Dis,
  Stats
    Admin: Dis, Oper: Dis
  CIR
    Admin (%): 0, Oper (Mbps): 0
  PIR
    Admin (%): 100, Oper (Mbps): 0

```

output definitions

QSAP	The QSet attachment point (QSAP) ID number. This is a logical entity generated internally by the switch to identify the association between a QSet instance and a port or link aggregate. The QSAP is not configurable at this time.
Parent	The parent QSAP ID. If the parent ID is different than the QSAP ID, then the port is a member of a link aggregate.
QSI	The QSet instance (QSI) ID number, internally generated by the switch.
QSP, Name, Admin, Oper	The QSet profile (QSP) ID number and name associated with the QSI. Also indicates the administrative and operational status of the QSP for the QSI.
WRP, Name, Admin, Oper	The WRED profile (WRP) ID number and name associated with the QSI. Also indicates the administrative and operational status of the WRP for the QSI. Only default WRP 1 is supported on the OS6900, and WRED is not supported on the OS10K.
Stats, Admin, Oper, Interval	The QSI administrative status, operational status, and time interval for statistics collection.
BW Admin (%)	The administrative percentage of bandwidth (currently not user-configurable).
BW Oper (Mbps)	The operational amount of bandwidth as determined by the port speed. For a link aggregate, this value is the sum of the operational bandwidths for the member ports.
QI 1-8	The queue scheduling and bandwidth configuration for each QSI queue. These values are determined by which one of the QSet profiles (QSP 1-4) is associated with the QSI.

Release History

Release 7.1.1; command was introduced.

Release 7.2.1; output display modified for the OmniSwitch 6900.

Release 7.2.1.R02; output display modified for the OmniSwitch 10K and OmniSwitch 6900.

Related Commands

qos qsi qsp	Changes the QSet profile association for a QSet instance.
qos qsi wred	Configures the administrative status of the WRED profile.
show qos qsi stats	Displays packet count statistics collected for a specific QSet instance.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsetInstanceTable
  alaVfcQsetId
  alaVfcQsetQsapId
  alaVfcQsetAdminState
  alaVfcQsetQSPId
  alaVfcQsetQSPName
  alaVfcQsetWRPId
  alaVfcQsetWRPName
  alaVfcQsetWRPAdminState
  alaVfcQsetWRPOperState
  alaVfcQsetSchedulingMethod
  alaVfcQsetStatsAdmin
  alaVfcQsetStatsOper
alaVfcQInstanceTable
  alaVfcQInstanceQId
  alaVfcQInstanceWRPAdminState
  alaVfcQInstanceWRPOperState
  alaVfcQInstanceWRPId
  alaVfcQInstanceWRPName
  alaVfcQInstanceCIRBandwidthLimitValue
  alaVfcQInstancePIRBandwidthLimitValue
  alaVfcQInstanceCIROperationalBandwidthLimitValue
  alaVfcQInstancePIROperationalBandwidthLimitValue
  alaVfcQInstanceStatsAdmin
  alaVfcQInstanceStatsOper
```

show qos qsi stats

Displays the total number of packets that flow through the QSet instance (QSI) queues associated with the specified port or link aggregate.

show qos qsi {**port** *slot/port[-port]* | **slot** *slot* | **linkagg** *agg_id[-agg_id]*} [**qi-id** *qi_id* | **qi** *qi_id*] **stats**

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>slot</i>	A slot number. Displays information for all ports on the slot.
<i>agg_id[-agg_id]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-15).
qi-id <i>qi_id</i>	The queue instance (QI) ID number. The valid range is 1–8. This parameter is supported only on the OmniSwitch 10K.
qi <i>qi_id</i>	The queue instance (QI) ID number. The valid range is 1–8. This parameter is supported only on the OmniSwitch 6900.

Defaults

By default, displays statistics for all QSet instances.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to display QSI statistics associated with specific ports or link aggregates.
- Use the **qi-id** *qi_id* or **qi** *qi_id* parameter to display statistics for a specific queue instance. There are eight queues associated with a single QSet instance. Each port and link aggregate is associated with one QSet instance.

Examples

```
-> show qos qsi port 1/7 stats
```

Port	Q	Total Tx	Total Drop
1/7	1	1566	0
1/7	2	24327553388	22977758468
1/7	3	0	0
1/7	4	0	0
1/7	5	0	0
1/7	6	40954875698	0
1/7	7	16	0
1/7	8	307882	0

```
-> show qos qsi port 1/7 qi 2 stats
```

Port	Q	Total Tx	Total Drop
1/7	2	24327553388	22977758468

output definitions

Port	The switch port.
QI	The egress queue ID (1–8) associated with the port.
Total TX	The total number of packets transmitted.
Total Drop	The total number of packets dropped.

Release History

Release 7.1.1; command was introduced.

Release 7.2.1; output display modified for the OmniSwitch 6900

Release 7.2.1.R02; output display modified for the OmniSwitch 10K and OmniSwitch 6900.

Related Commands

qos qsi stats	Configures the statistics collection administrative status and interval for the specified QSet instance.
show qos qsi stats rate	Displays the number of packets per second that flow through the QSI queues.
show qos qsi stats bytes	Displays the total number of bytes that flow through the QSI queues.
clear qos qsi stats	Clears statistics collected for one or more QSet instances.

MIB Objects

```
alcatelIND1VfcMIB
  alaVfcQsetInstanceTable
    alaVfcQsetId
    alaVfcQsetQsapId
    alaVfcQsetAdminState
    alaVfcQsetQSPId
    alaVfcQsetQSPName
    alaVfcQsetWRPId
    alaVfcQsetWRPName
    alaVfcQsetWRPAdminState
    alaVfcQsetWRPOperState
    alaVfcQsetSchedulingMethod
    alaVfcQsetStatsAdmin
    alaVfcQsetStatsOper
  alaVfcQInstanceTable
    alaVfcQInstanceQId
    alaVfcQInstanceWRPAdminState
    alaVfcQInstanceWRPOperState
    alaVfcQInstanceWRPId
    alaVfcQInstanceWRPName
    alaVfcQInstanceCIRBandwidthLimitValue
    alaVfcQInstancePIRBandwidthLimitValue
```

```
alaVfcQInstanceCIROperationalBandwidthLimitValue  
alaVfcQInstancePIROperationalBandwidthLimitValue  
alaVfcQInstanceStatsAdmin  
alaVfcQInstanceStatsOper  
alaVfcQInstancePacketsEnqueued  
alaVfcQInstancePacketsDequeued  
alaVfcQInstancePacketsDropped  
alaVfcQInstanceGreenPacketsAccepted  
alaVfcQInstanceGreenPacketsDropped  
alaVfcQInstanceYellowPacketsAccepted  
alaVfcQInstanceYellowPacketsDropped  
alaVfcQInstanceRedPacketsAccepted  
alaVfcQInstanceRedPacketsDropped
```

show qos qsi stats rate

Displays the number of packets per second that flow through the QSet instance (QSI) queues.

```
show qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} [qi qi_id] stats rate [bytes]
```

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>slot</i>	A slot number. Displays information for all ports on the slot.
<i>agg_id[-agg_id]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-15).
qi <i>qi_id</i>	The queue instance (QI) ID number. The valid range is 1–8.
bytes	Displays the number of bytes per second, instead of the number of packets per second.

Defaults

By default, displays the number of packets per second for all the QSI queues.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to display QSI statistics associated with specific ports or link aggregates.
- Use the **qi** *qi-id* parameter to display statistics for a specific queue instance. There are eight queues associated with a single QSet instance. Each port and link aggregate is associated with one QSet instance.

Examples

```
-> show qos qsi port 1/7 stats rate
```

Port	Q	Average Tx/s	Average Drop/s
1/7	1	0	0
1/7	2	8956	3177031
1/7	3	0	0
1/7	4	0	0
1/7	5	0	0
1/7	6	3186422	0
1/7	7	0	0
1/7	8	1	0

```

-> show qos qsi port 1/1 qi 2 stats rate
          Port          Q          Average          Average
          Port          Q          Tx/s          Drop/s
-----+-----+-----+-----+
1/7          2          8956          3177031

-> show qos qsi port 1/7 stats rate bytes
          Port          Q          Average          Average
          Port          Q          Tx/s          Drop/s
-----+-----+-----+-----+
1/7          1          0          0
1/7          2          3254839          1151070600
1/7          3          0          0
1/7          4          0          0
1/7          5          0          0
1/7          6          1154619451          0
1/7          7          0          0
1/7          8          349          0

-> show qos qsi port 1/7 qi 2 stats rate bytes
          Port          Q          Average          Average
          Port          Q          Tx/s          Drop/s
-----+-----+-----+-----+
1/7          2          3254839          1151070600

```

output definitions

Port	The switch port.
QI	The egress queue ID (1–8) associated with the port.
Total TX	The number of packets or bytes transmitted per second.
Total Drop	The number of packets or bytes dropped per second.

Release History

Release 7.2.1; command was introduced

Related Commands

show qos qsi Displays the QSet instance configuration.

clear qos qsi stats Clears statistics collected for one or more QSet instances.

MIB Objects

```

alcatelIND1VfcMIB
  alaVfcQInstanceTable
    alaVfcQInstanceQId
    alaVfcQInstancePacketsEnqueued
    alaVfcQInstanceBytesEnqueued
    alaVfcQInstancePacketsDropped
    alaVfcQInstanceBytesDropped

```

show qos qsi stats bytes

Displays the total number of bytes that flow through the QSet instance (QSI) queues.

show qos qsi {*port slot/port[-port]* | *slot slot* | *linkagg agg_id[-agg_id]*} [*qi qi_id*] **stats bytes**

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>slot</i>	A slot number. Displays information for all ports on the slot.
<i>agg_id[-agg_id]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-15).
<i>qi qi_id</i>	The queue instance (QI) ID number. The valid range is 1–8.

Defaults

By default, displays the total number of bytes for each of the QSI queues.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to display QSI statistics associated with specific ports or link aggregates.
- Use the **qi** *qi-id* parameter to display statistics for a specific queue. There are eight queues associated with each QSet instance. Each port and link aggregate is associated with one QSet instance.

Examples

```
-> show qos qsi port 1/7 stats bytes
```

Port	Q	Total Tx	Total Drop
1/7	1	389250	0
1/7	2	8803326761200	8467375458000
1/7	3	0	0
1/7	4	0	0
1/7	5	0	0
1/7	6	14972813873924	0
1/7	7	1072	0
1/7	8	108256218	0

```
-> show qos qsi port 1/7 qi 2 stats bytes
```

Port	Q	Total Tx	Total Drop
1/7	2	8803326761200	8467375458000

output definitions

Port	The switch port.
QI	The egress queue ID (1–8) associated with the port.
Total TX	The total number of bytes transmitted.
Total Drop	The total number of bytes dropped.

Release History

Release 7.2.1; command was introduced.

Related Commands

show qos qsi	Displays the QSet instance configuration.
clear qos qsi stats	Clears statistics collected for one or more QSet instances.

MIB Objects

```
alcatelIND1VfcMIB
  alaVfcQInstanceTable
    alaVfcQInstanceQId
    alaVfcQInstancePacketsEnqueued
    alaVfcQInstanceBytesEnqueued
    alaVfcQInstancePacketsDropped
    alaVfcQInstanceBytesDropped
```

output definitions

Port	The switch port.
Q	The egress queue ID (1–8) associated with the port.
Green TX, Green Drop	The number of green packets or bytes transmitted and dropped.
Yellow TX, Yellow Drop	The number of yellow packets or bytes transmitted and dropped.
Red TX, Red Drop	The number of red packets or bytes transmitted and dropped.

Release History

Release 7.2.1.R01; WRED per Q stats not supported; Tx stats not supported.

Related Commands

show qos qsi	Displays the QSet instance configuration.
clear qos qsi stats	Clears statistics collected for one or more QSet instances.

MIB Objects

```

alcatelIND1VfcMIB
  alaVfcQInstanceTable
    alaVfcQInstanceQId
    alaVfcQInstanceGreenPacketsAccepted
    alaVfcQInstanceGreenBytesAccepted
    alaVfcQInstanceGreenPacketsDropped
    alaVfcQInstanceGreenBytesDropped
    alaVfcQInstanceYellowPacketsAccepted
    alaVfcQInstanceYellowBytesAccepted
    alaVfcQInstanceYellowPacketsDropped
    alaVfcQInstanceYellowBytesDropped
    alaVfcQInstanceRedPacketsAccepted
    alaVfcQInstanceRedBytesAccepted
    alaVfcQInstanceRedPacketsDropped
    alaVfcQInstanceRedBytesDropped

```

clear qos qsi stats

Clears QSet instance (QSI) statistics.

```
clear qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} [qi-id qi_id] stats
```

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>slot</i>	A slot number. Displays information for all ports on the slot.
<i>agg_id[-agg_id]</i>	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
<i>qi-id</i>	The queue instance (QI) ID number. The valid range is 1–8.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **port** *slot/port*, **slot** *slot*, and **linkagg** *agg_id* parameters to clear QSI statistics associated with specific ports or link aggregates.
- Use the **qi-id** *qi_id* parameter to clear statistics for a specific queue instance. There are eight queues associated with a single QSet instance.

Examples

```
-> clear qos qsi port 1/2 qi-id 3 stats
-> clear qos qsi linkagg 10 stats
-> clear qos qsi linkagg 5 qi-id 8 stats
-> clear qos qsi slot 2 stats
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show qos qsi stats](#)

Displays QSet instance statistics.

MIB Objects

```
alcatelIND1VfcMIB
alaVfcQsapTable
  alaVfcQsapClearStats
  alaVfcQsapQpId
```

qos qsp dcb import

Imports a Data Center Bridging profile (DCB) to a new or previous custom profile.

```
qos qsp dcb {dcp_id | dcp_name} import qsp dcb {import_dcp_id | import_dcp_name} [802.3x-pause]
```

```
no qos qsp dcb {dcp_id | dcp_name}
```

Syntax Definitions

<i>dcp_id</i>	A DCB custom profile ID. The valid custom profile ID range is 11 through 128.
<i>dcp_name</i>	The DCB profile name.
<i>import_dcp_id</i>	The ID of the DCB profile to import. The valid profile ID range is 1–10 to specify a predefined profile and 11–128 to specify a custom profile.
<i>import_dcp_name</i>	The name of the DCB profile to import.
802.3x-pause	Makes the profile pause-ready. When enabled, the Priority based Flow Control (PFC) is lossy for all traffic classes in the profile and they cannot be changed to lossless.

Defaults

By default the **802.3x-pause** flag is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The new DCB profile must be unique and not contain the same name and ID of an existing DCB profile.
- Use the **no** form of the command to remove an existing custom DCB profile.
- The pre-defined DCB profiles from 1 to 10 cannot be removed.
- A custom profile attached to a port cannot be removed. In this case the profile must be disassociated from the port before being removed.
- Use the **802.3x-pause** tag to enable pause-ready on the profile. When enabled, the PFC is lossy for all traffic classes in the profile and they cannot be changed to lossless. It can be applied to ports where pause can be configured instead of PFC. If the port has a regular DCB profile attached, PFC TLV and PFC willing must be disabled on the port before the pause-ready profile is applied.

Examples

```
-> qos qsp dcb 33 import qsp dcb 8
-> qos qsp dcb lossyETS import qsp 10
-> qos qsp dcb 34 import qsp dcb 7 802.3x-pause
-> no qsp dcb 33
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsp dcb	Displays the configured DCB profile and the traffic classes associated to the DCB profile.
show qos qsi stats	Displays the queue statistics for DCB and (Non-DCB) NDCB ports.
clear qos qsi dcb pfc stats	Clears the port statistics.

MIB Objects

```
alaDcbxDCProfileTable  
  alaDcbxDCPID  
  alaDcbxDCPName  
  alaDcbxDCPTemplateDCPID  
  alaDcbxDCPTemplateDCPName  
  alaDcbxDCP8023xPauseReady  
  alaDcbxDCPRowStatus
```

qos qsp dcb tc

Modifies the Data Center Bridging (DCB) traffic class attributes of a DCB profile.

```
qos qsp dcb {dcp_id | dcp_name} tc tc_num
{
  pfc flow-type { ll | nll} |
  pfc link-delay allowance |
  min-bw % |
  max-bw % |
  recommended bw %
}
```

Syntax Definitions

<i>dcp_id</i>	A DCB custom profile ID. The valid custom profile ID range is 11 through 128.
<i>dcp_name</i>	The DCB custom profile name.
<i>tc_num</i>	The traffic class number in the DCB profile.
ll	Designates traffic class as lossless.
nll	Designates traffic class as non-lossless (lossy).
<i>allowance</i>	Link delay allowance value for PFC.
min-bw %	Sets the minimum bandwidth guaranteed for the Enhanced Transmission Selection (ETS) traffic class.
max-bw %	Sets the maximum bandwidth guaranteed for the Strict Priority (SP) traffic class.
recommended bw %	Sets the recommended minimum bandwidth for the traffic class.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **pfc flow-type** option allows to change a traffic class from lossless (ll) to lossy (nll) or lossy (nll) to lossless (ll).
- The **pfc link-delay** option allows to set the actual headroom for the traffic class. Incorrect setting can result in traffic loss.
- The **min-bw** option allows to set the minimum bandwidth guaranteed for the ETS traffic class.
- The **max-bw** option allows to set the maximum bandwidth guaranteed for the SP traffic class.

- The **recommended bw** option allows to set the recommended minimum bandwidth for the traffic class.

Examples

```
-> qos qsp dcb 11 tc 0 min-bw 3
-> qos qsp dcb lossyETS tc 1 min-bw 12
-> qos qsp dcb lossyETS tc 2 pfc flow-type 11
-> qos qsp dcb 11 tc 0 recommended bw 3
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsp dcb Displays the configured DCB profiles and the traffic classes associated to the DCB profile.

MIB Objects

```
alaDcbxDCPTrafficClassTable
  alaDcbxDCPTDCPId
  alaDcbxDCPTCTrafficClass
  alaDcbxDCPTDCPName
  alaDcbxDCPTCPFCTrafficFlow
  alaDcbxDCPTCPFCLinkDelay
  alaDcbxDCPTCMinimumBandwidth
  alaDcbxDCPTCMaximumBandwidth
  alaDcbxDCPTCRecommendedBandwidth
```

qos qsp dcb tc-numbering

Modifies the traffic class (TC) numbering for custom profiles.

```
qos qsp dcb {dcp_id | dcp_name} tc-numbering tc_num
```

Syntax Definitions

<i>dcp_id</i>	A DCB custom profile ID. The valid custom profile ID range is 11 through 128.
<i>dcp_name</i>	The DCB custom profile name.
<i>tc_num</i>	Enter the traffic class numbering sequence for the DCB profile.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The command can be used to modify the traffic class numbering for the custom profiles.
- The numbering must be assigned in ascending order. For example, a profile with TCs numbered 0, 1, 2, can be changed to 1, 5, 7.
- The number of TCs specified must match the number of TCs in the profile.

Examples

```
-> qos qsp dcb 11 tc-numbering 1 5 7 9
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show qos qsp dcb](#) Displays the configured DCB profiles and the traffic classes associated to the DCB profile.

MIB Objects

```
alaDcbxDCProfileTable  
  alaDcbxDCPTDCPName  
  alaDcbxDCPTCsPresent
```

show qos qsp dcb

Displays the configured DCB profiles and the traffic classes associated to the DCB profile.

show qos qsp dcb [*dcp_id* | *dcp_name*] [**tc** *tc_num*]

Syntax Definitions

<i>dcp_id</i>	DCB profile ID. DCB profile ID 11–128 refers to the custom profiles. DCB profile ID 1–0 refers to the predefined profiles.
<i>dcp_name</i>	DCB profile name.
<i>tc_num</i>	The traffic class associated to the DCB profile. The valid range is 0–7.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command displays the details of the configured DCB profile.
- Use the **tc** option to display the traffic classes associated to the DCB profile.

Examples

```
-> show qos qsp dcb
```

Legends: Prio TC Map:

Represents the priority to traffic class mapping;
begins with priority 0 on the left and displays the
traffic class it belongs to.

#	Name	Priority TC Map	PFC Cap	ETS		Template-DCP	802.3x Pause-Ready
				Max	TC		
1	dcp-1	00001122	8	8	1	dcp-1	No
2	dcp-2	00112233	8	8	2	dcp-2	No
3	dcp-3	00112234	8	8	3	dcp-3	No
4	dcp-4	10223345	8	8	4	dcp-4	No
5	dcp-5	10234456	8	8	5	dcp-5	No
6	dcp-6	10234567	8	8	6	dcp-6	No
7	dcp-7	01234567	8	8	7	dcp-7	No
8	dcp-8	01234567	8	8	8	dcp-8	No
9	dcp-9	10234567	8	8	9	dcp-9	No
10	dcp-10	10234567	8	8	10	dcp-10	No
20	dcp-20	10234567	8	8	10	dcp-10	No

output definitions

#	Indicates a DCB profile entry.
Name	Name of the DCB profile.
Priority TC Map	Indicates the priority of the traffic class.
PFC Cap	Indicates the number of traffic classes on the local device that have simultaneously PFC enabled.
ETS Max TC	Indicates the number of traffic classes supported.
Template-DCP #	Identifies the template DCB profile.
Template-DCP Name	Name of the template DCB profile.
802.3x Pause-Ready	Indicates if pause-ready is enabled for the profile.

-> show qos qsp dcp tc

Legends: Linkdelay shown in KB.
 * denotes user modified value

#	Name	TC	Priorities	ETS		ETS Sched	ETS		PFC Mode	PFC LinkDelay
				Min BW	Max BW		Reco BW	Reco Sched		
1	Dft_1	0	4567	0	100	SP	0	SP	nLL	0
1	Dft_1	1	23	50	100	ETS	50	ETS	LL	80*
1	Dft_1	2	01	50	100	ETS	50	ETS	LL	60

output definitions

#	Indicates a DCB profile entry.
Name	Name of DCB profile.
TC	Indicates the traffic class.
Priorities	Indicates the priorities assigned to the traffic class.
ETS Min BW	Indicates the minimum bandwidth assigned to the traffic class.
ETS Max BW	Indicates the maximum bandwidth assigned to the traffic class.
ETS Sched	Indicates the traffic class scheduler assigned to the traffic class.
ETS Reco BW	Indicates the recommended minimum bandwidth assigned to the traffic class.
ETS Reco Sched	Indicates the recommended traffic class scheduler assigned to the traffic class.
PFC Mode	Indicates if PFC traffic flow is enabled on the traffic class.
PFC LinkDelay	Indicates the delay in the PFC link.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsp dcb import	Imports a data center profile to a new or old custom DCB profile.
clear qos qsi stats	Modifies the Data Center Bridging Capabilities Exchange Protocols (DCBX) control portion of a DCB profile.
qos qsp dcb tc	Modifies the Data Center Bridging (DCB) attributes of a DCB profile.
qos qsp dcb tc-numbering	Modifies the priority of traffic class mapping the custom profiles.
clear qos qsi dcb pfc stats	Clears the port statistics.

MIB Objects

```

alaDcbxDCProfileTable
  alaDcbxDCPId
  alaDcbxDCPName
  alaDcbxDCPPriorityTCMap
  alaDcbxDCPPFCCap
  alaDcbxDCPETSTrafficClassesSupported
  alaDcbxDCPTemplateDCPId
  alaDcbxDCPTemplateDCPName
  alaDcbxDCP8023xPauseReady
alaDcbxDCPTrafficClassTable
  alaDcbxDCPTCDCPId
  alaDcbxDCPTDCPName
  alaDcbxDCPTCTrafficClass
  alaDcbxDCPTCPriorityMap
  alaDcbxDCPTCMinimumBandwidth
  alaDcbxDCPTCMaximumBandwidth
  alaDcbxDCPTCTrafficScheduler
  alaDcbxDCPTCRecommendedBandwidth
  alaDcbxDCPTCRecommendedTrafficScheduler
  alaDcbxDCPTCPFCTrafficFlow
  alaDcbxDCPTCPFCLinkDelay

```

qos qsi dcb dcbx admin-state

Enables or disables DCB exchange protocol (DCBX) functionality on a per port basis.

```
qos qsi {port slot/port[-port] | linkagg agg[-agg]} dcb dcbx admin-state {enable | disable}
```

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>agg[-agg]</i>	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
enable	Enables the DCBX functionality on the port.
disable	Disables the DCBX functionality on the port.

Defaults

parameter	default
dcbx admin-state	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The DCBX admin-state, enables or disables DCBX TLVs and negotiation on a port.

Examples

```
-> qos qsi port 1/10 dcb dcbx admin-state enable
-> qos qsi port 1/10 dcb dcbx admin-state disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi qsp dcb

Assigns a DCB profile to a port.

qos qsi dcb dcbx ets

Enables or disables application Type, Length, Value (TLV) transmission on a per port basis.

show qos qsi dcbx

Displays the configured ports in the system and the related DCBX information.

MIB Objects

alaDcbxPortInstanceEntry

alaDcbxPIIfIndex

alaDcbxPIDCBXAdmin

qos qsi qsp dcb

Assigns a DCB profile to a port or link aggregate.

```
qos qsi {port slot/port[-port] | linkagg agg[-agg]} qsp dcb {dcp_id | dcb_name}
```

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>agg[-agg]</i>	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
<i>dcp_id</i>	DCB profile ID. DCB profile ID 11 through 128 refers to the custom profiles. DCB profile ID 1 through 10 refers to the predefined profiles.
<i>dcb_name</i>	DCB profile name.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When a DCB profile is assigned to a linkagg, all the ports associated to the linkagg will be applied with the DCB profile.
- Avoid configuring different profiles for each port of the linkagg.
- The command will not work if the linkagg is associated with 1Gig port. Different combination of ports (10G and 40G) are allowed in a linkagg.

Examples

```
-> qos qsi port 1/11 qsp dcb lossyETS  
-> qos qsi port 1/11 qsp dcb 7
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsi stats

Displays the queue statistics for DCB and NDCB ports.

clear qos qsi dcb pfc stats

Clears the port statistics.

MIB Objects

alaDcbxPortInstanceEntry

alaDcbxPIAdminDCPIId

alaDcbxPIAdminDCPName

show qos qsi dcbx

Displays the DCBX port configuration and status.

```
show qos qsi [port slot/port[-port2] | linkagg agg_id[-agg_id2]] dcb dcbx [status]
```

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>agg_id[-agg_id2]</i>	A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
status	Displays the DCBX operational status for the port.

Defaults

By default, the DCBX configuration is displayed for all ports.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the *slot/port* or *agg_id*, parameters to display information for a specific port or link aggregate.
- Use the **status** option to display the status information of the DCBX related to the port.

Examples

```
-> show qos qsi port 1/1-4 dcb dcbx
```

Port	DCP Name	DCBX Admin	Stats Admin	PFC Defense	PFC TLV	PFC Will	Cfg TLV	Reco TLV	ETS Will	App TLV
1/1	1 dcp-1	Ena	Dis	Dis	Ena	Yes	Ena	Ena	Yes	Ena
1/2	1 dcp-1	Ena	Dis	Dis	Ena	Yes	Ena	Ena	Yes	Ena
1/3	1 dcp-1	Ena	Dis	Dis	Ena	Yes	Ena	Ena	Yes	Ena
1/4	2 dcp-2	Dis	Dis	Dis	Ena	Yes	Ena	Ena	Yes	Ena

output definitions

Port	Configured DCB ports.
DCP Name	Identifies the DCB profile assigned to the port.
DCBX Admin	Indicates the admin status of the DCBX on the port.
Stats Admin	Indicates if gathering statistics is enabled or disabled on the port.

output definitions (continued)

PFC Defense	Indicates the status of PFC defense. Applies when PFC negotiation fails. If value is enabled, then PFC becomes disabled but traffic still flows. If the value is disabled, then PFC local configuration remains on the port.
PFC TLV	Indicates whether the IEEE 802.1 organizationally defined PFC TLV transmission is allowed on a given LLDP transmission capable port.
PFC Will	Indicates whether the port is willing to accept the remote peer's PFC configuration.
Cfg TLV	Indicates whether ETS configuration TLV transmission is allowed on a port.
Reco TLV	Indicates whether ETS configuration TLV transmission is allowed on a port.
ETS Will	Indicates whether the port is willing to accept the remote peer's ETS recommended configuration.
App TLV	Indicates whether the IEEE 802.1 organizationally defined Application Priority TLV transmission is allowed on a given LLDP transmission capable port.

```
-> show qos qsi port 1/1-5 dcb dcbx status
```

Port	DCBX Oper	Local		Error	Action
		Oper	Changed		
1/1	Ena	Yes		PFC Resources Exhausted	Disabled PFC
1/2	Ena	No		PFC TLV Mismatch	Restored PFC admin config
1/3	Ena	Yes		ETS TLV Mismatch	Restored ETS admin config
1/4	Ena	Yes		OK	n/a
1/5	Ena	No		PFC and ETS TLV Mismatch	Restored ETS and PFC admin config

output definitions

Port	Configured DCB ports.
DCBX Oper	Indicates the DCBX operation status on the port.
Local Oper Changed	Identifies if the local configuration is different from the configuration imported from the DCB profile applied to the port.
Error	Indicates the port status.
Action	Indicates the action taken as a result of the status.

Release History

Release 7.3.1; command was introduced.

Related Commands

- qos qsi qsp dcb** Assigns a DCB profile to a port or link aggregate.
- qos qsi dcb dcbx admin-state** Enables or disables DCBX functionality on a per port basis.

MIB Objects

```
alaDcbxPortInstanceTable  
  alaDcbxPIIfIndex  
  alaDcbxPIAdminDCPId  
  alaDcbxPIAdminDCPName  
  alaDcbxPIDCBXAdmin  
  alaDcbxPIStatsAdmin  
  alaDcbxPIPFCDefense  
  lldpXdot1dcbxConfigPFCTxEnable  
  lldpXdot1dcbxConfigETSConfigurationTxEnable  
  lldpXdot1dcbxConfigETSRecommendationTxEnable  
  lldpXdot1dcbxConfigApplicationPriorityTxEnable
```

show qos qsi summary

Displays the summary of the user ports in the switch.

show qos qsi {port slot/port[-port] | linkagg agg_id[-agg_id]} summary

Syntax Definitions

slot/port[-port] A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

agg_id[-agg_id] A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays the summary of the user ports in the switch.

Examples

```
-> show qos qsi port 1/1-5 summary
```

Legends: * indicates port is misconfigured.

Port	Profile		Mode	Parent
	#	Name		
1/1	8	dcp-8	DCB	1/1
1/2	8	dcp-8	DCB	1/2
1/3	8	dcp-8	DCB	1/3
1/4	1	dcp-1	DCB	1/4
1/5	1	dcp-1	DCB	1/5

output definitions

Port	Configured DCB ports.
Profile #	Identifies the DCB profile assigned to the port.
Profile Name	Name of the DCB profile assigned to the port.
Mode	Indicates if the port is DCB or NDCB.
Parent	Lists the parent of the port.

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsi dcbx

Displays the configured ports in the system and the related DCBX information.

qos qsi qsp dcb

Assigns a DCB profile to a port or link aggregate.

MIB Objects

alaVfcQsetInstanceTable

alaVfcQsetId

alaVfcQsetQSPID

alaVfcQsetQSPName

alaDcbxPortInstanceTable

alaVfcQsapParent

qos qsi dcb dcbx ets

Enables or disables config-TLV, recommended-TLV, and the willing bit for ETS on a per-port basis.

qos qsi {port *slot/port[-port2]* | linkagg *agg[-agg2]*} **dcb dcbx ets** [**config-tlv** {enable | disable} | **recommend-tlv** {enable | disable} | **willing** {yes | no}]

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>agg[-agg]</i>	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
config-tlv enable	Enables the transmission of ETS configuration TLVs.
config-tlv disable	Disables the transmission of ETS configuration TLVs.
recommend-tlv enable	Enables the transmission of ETS recommended TLVs.
recommend-tlv disable	Disables the transmission of ETS recommended TLVs.
yes	Sets the willing bit to on in the TLVs.
no	Sets the willing bit to off in the TLVs.

Defaults

parameter	default
config-tlv {enable disable}	enable
ets recommend-tlv {enable disable}	enable
willing {yes no}	yes

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the option **ets config-tlv** to enable or disable the transmission of ETS configuration TLVs. To use this option, DCBX must be enabled on the port.
- Use the option **ets recommended-tlv** to enable or disable the transmission of ETS recommended TLVs. To use this option, DCBX must be enabled on the port.
- Use the option **ets willing** to set the willing bit on the TLVs. This option is used when the DCBX is enabled on the port and the ETS configuration TLV is sent on the port.

Examples

```
-> qos qsi port 1/1-10 dcb dcbx ets config-tlv disable
-> qos qsi port 1/11 dcb dcbx ets recommended-tlv disable
-> qos qsi linkagg 5 dcb dcbx ets willing no
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show qos qsi dcb ets](#)

Displays the configured ports in the system and the related DCBX ETS and ETS traffic class information.

MIB Objects

```
lldpXdot1dcbxConfigETSConfigurationTable  
lldpXdot1dcbxConfigETSRecommendationTable  
lldpXdot1dcbxLocETSBasicConfigurationTable  
    lldpXdot1dcbxConfigETSConfigurationTxEnable  
    lldpXdot1dcbxConfigETSRecommendationTxEnable  
    lldpXdot1dcbxLocETSConWilling
```

show qos qsi dcb ets

Displays the configured ports in the system and the related DCBX ETS and ETS traffic class information.

```
show qos qsi {port slot/port[-port] | linkagg agg[-agg]} dcb ets [tc [tc_num]]
```

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>agg[-agg]</i>	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
<i>tc_num</i>	Enter the traffic class for which the information needs to be displayed. The valid range is 0-7.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *tc_num* option to display the DCBX ETS information for a specific traffic class.

Examples

```
-> show qos qsi port 1/1 dcb ets
```

Legends: Prio TC Map:

Represents the priority to traffic class mapping;
begins with priority 0 on the left and displays the
traffic class it belongs to.

* indicates port oper status is different than the configured status

Port	Loc-Adm				Loc-Oper				Rem-Oper			
	Prio	Max	CBS	Will	Prio	Max	CBS	Will	Prio	Max	CBS	Will
1/1	00111222	3	Dis	Yes	00111222	3	Dis	Yes	00111222	3	Ena	Ena

output definitions

Port	Configured DCB ports.
Loc-Adm Prio TC Map	Indicates the traffic class to which the priority is to be assigned.
Loc-Adm Max TC	Indicates the number of traffic classes supported.
Loc-Adm CBS	Indicates the status of the credit-based shaper traffic support.
Loc-Adm Will	Indicates if the local system is willing to accept the ETS configuration recommended by the remote system.
Loc-Oper Prio TC Map	Indicates the traffic class the priority belongs to.

output definitions (continued)

Loc-Oper Max TC	Indicates the number of traffic classes supported in the local system.
Loc-Oper CBS	Indicates if the credit-based shaper traffic is supported on the local system.
Loc-Oper Will	Indicates if the credit-based shaper traffic selection is supported on the local system.
Rem-Oper Prio TC Map	Indicates the priority that is assigned to a traffic class.
Rem-Oper Max TC	Indicates the number of traffic classes supported in the remote system.
Rem-Oper CBS	Indicates if the credit-based shaper traffic selection is supported on the remote system.
Rem-Oper Will	Indicates if the remote system is willing to accept the ETS configuration recommended by the remote system.

-> show qos qsi port 1/1 dcb ets tc

Legends: * indicates port oper status is different than the configured status

Port	TC	Loc-Adm		Loc-Adm		Loc-Oper		Loc-Oper		Loc-Oper		Rem-Oper		Rem-Reco	
		Priorities	BW	Sched	BW	Sched	Priorities	BW	Sched	BW	Sched	Priorities	BW	Sched	
1/1	0	01	0	SP	0	SP	01	0	SP	0	SP	01	0	SP	
1/1	1	23	50	ETS	50	ETS	23	50	ETS	50	ETS	23	50	ETS	
1/1	2	4567	50	ETS	50	ETS	4567	50	ETS	50	ETS	4567	50	ETS	

output definitions

Port	Configured DCB ports.
TC	Indicates the traffic class the priority belongs to.
Loc-Adm Priorities	Indicates the priority assigned to the traffic class in the local system.
Loc-Adm BW	Indicates the bandwidth assignment to the traffic class in the local system.
Loc-Adm Sched	Indicates the traffic selection assignment to the traffic class in the local system.
Loc-Adm Reco BW	Indicates the traffic class to bandwidth assignment in the local system.
Loc-Adm Reco Sched	Indicates the traffic class to traffic selection assignment in the local system.
Loc-Oper Priorities	Indicates the priority assigned to the traffic class in the local system.
Loc-Oper BW	Indicates the bandwidth assigned to the traffic class in the local system.
Loc-Oper Sched	Indicates the traffic class to traffic selection assignment in the local system.
Loc-Oper Reco BW	Indicates the traffic class to bandwidth assignment in the local system.
Loc-Oper Reco Sched	Indicates the priority to traffic selection assignment in the local system.
Rem-Oper Priorities	Indicates the priority assigned to the traffic class in the remote system.
Rem-Oper BW	Indicates the traffic class to bandwidth assignment in the remote system.
Rem-Oper Sched	Indicates the traffic class to traffic selection assignment in the remote system.

output definitions (continued)

Rem-Oper Reco BW	Indicates the traffic class to bandwidth assignment in the remote system.
Rem-Oper Reco Sched	Indicates the priority to traffic selection assignment in the remote system.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi dcb dcbx ets Enables or disables config-tlv, recommended-tlv, and willing for ETS on a per port basis.

MIB Objects

```

lldpXdot1dcbxAdminETSConPriorityAssignmentTable
lldpXdot1dcbxAdminETSBasicConfigurationTable
lldpXdot1dcbxLocETSConPriorityAssignmentTable
lldpXdot1dcbxLocETSBasicConfigurationTable
lldpXdot1dcbxRemETSConPriorityAssignmentTable
lldpXdot1dcbxRemETSBasicConfigurationTable
  lldpV2LocPortIfIndex
  lldpXdot1dcbxAdminETSConPriTrafficClass
  lldpXdot1dcbxAdminETSConTrafficClassesSupported
  lldpXdot1dcbxAdminETSConCreditBasedShaperSupport
  lldpXdot1dcbxAdminETSConWilling
  lldpXdot1dcbxLocETSConPriTrafficClass
  lldpXdot1dcbxLocETSConTrafficClassesSupported
  lldpXdot1dcbxLocETSConCreditBasedShaperSupport
  lldpXdot1dcbxLocETSConWilling
  lldpXdot1dcbxRemETSConPriTrafficClass
  lldpXdot1dcbxRemETSConTrafficClassesSupported
  lldpXdot1dcbxRemETSConCreditBasedShaperSupport
  lldpXdot1dcbxRemETSConWilling
lldpXdot1dcbxAdminETSConTrafficClassBandwidthTable
lldpXdot1dcbxAdminETSConTrafficSelectionAlgorithmTable
lldpXdot1dcbxAdminETSRecoTrafficClassBandwidthTable
lldpXdot1dcbxAdminETSRecoTrafficSelectionAlgorithmTable
lldpXdot1dcbxLocETSConTrafficClassBandwidthTable
lldpXdot1dcbxLocETSConTrafficSelectionAlgorithmTable
lldpXdot1dcbxLocETSRecoTrafficClassBandwidthTable
lldpXdot1dcbxLocETSRecoTrafficSelectionAlgorithmTable
lldpXdot1dcbxRemETSConTrafficClassBandwidthTable
lldpXdot1dcbxRemETSConTrafficSelectionAlgorithmTable
lldpXdot1dcbxRemETSRecoTrafficClassBandwidthTable
lldpXdot1dcbxRemETSRecoTrafficSelectionAlgorithmTable
  lldpV2LocPortIfIndex
  lldpXdot1dcbxAdminETSConTrafficClass

```

```
lldpXdot1dcbxAdminETSConTrafficClassBandwidth
lldpXdot1dcbxAdminETSConTrafficSelectionAlgorithm
lldpXdot1dcbxAdminETSRecoTrafficClassBandwidth
lldpXdot1dcbxAdminETSRecoTrafficSelectionAlgorithm
lldpXdot1dcbxLocETSConTrafficClassBandwidth
lldpXdot1dcbxLocETSConTrafficSelectionAlgorithm
lldpXdot1dcbxLocETSRecoTrafficClassBandwidth
lldpXdot1dcbxLocETSRecoTrafficSelectionAlgorithm
lldpXdot1dcbxRemETSConTrafficClassBandwidth
lldpXdot1dcbxRemETSConTrafficSelectionAlgorithm
lldpXdot1dcbxRemETSRecoTrafficClassBandwidth
lldpXdot1dcbxRemETSRecoTrafficSelectionAlgorithm
```

qos qsi dcb dcbx pfc

Enables or disables config-TLV, defense mode, and willing for PFC on a per port basis.

```
qos qsi {port slot/port[-port] | linkagg agg[-agg]} dcb dcbx pfc [config-tlv {enable | disable} | defense {enable | disable} | willing {yes | no}]
```

Syntax Definitions

<i>slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
<i>agg[-agg]</i>	The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
config-tlv enable	Enables the transmission of PFC configuration TLVs.
config-tlv disable	Disables the transmission of PFC configuration TLVs.
defense enable	Enables the defense mode for the PFC.
defense disable	Disables the defense mode for the PFC.
willing yes	Allows the PFC to negotiate with the network.
willing no	Stops the PFC from negotiating with the network.

Defaults

parameter	default
pfc config-tlv	enable
pfc defense	enable
pfc willing	yes

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the option **pfc config-tlv** to enable or disable the transmission of PFC configuration TLVs. To use this option, DCBX must be enabled on the port.
- Use the option **ets willing** to allow the PFC to negotiate with the network.

Examples

```
-> qos qsi port 1/1-10 dcb dcbx pfc config-tlv disable
-> qos qsi port 1/11 dcb dcbx pfc defense disable
-> qos qsi linkagg 5 dcb dcbx pfc willing no
```

Release History

Release 7.3.1; command was introduced.

Related Commands

- show qos qsi dcbx pfc** Displays the configured ports in the system and the related DCBX PFC information.
- show qos pfc-lossless-usage** Displays the usage of the PFC lossless traffic class on the switch.
- show qos qsi dcb pfc stats** Displays the traffic statistics per port and per traffic class.

MIB Objects

```
lldpXdot1dcbxConfigPFCTable  
  lldpXdot1dcbxConfigPFCTxEnable  
  alaDcbxPIPFCDefense  
  lldpXdot1dcbxLocPFCWilling
```

show qos qsi dcbx pfc

Displays the configured ports in the system and the related DCBX PFC information.

show qos qsi {port slot/port[-port] | linkagg agg[-agg]} dcb pfc

Syntax Definitions

slot/port[-port] A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

agg[-agg] The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If there is no PFC TLV received from the remote end, then the remote information will be blank.

Examples

```
-> show qos qsi port 4/1-2 dcb pfc
```

Legends: * indicates port oper status is different than the configured status

Port	Loc-Adm Priorities	Loc-Adm				Loc-Oper				Rem-Oper			
		MBC	Will	Cap	Priorities	MBC	Will	Cap	Priorities	MBC	Will	Cap	
4/1*	0467	No	Yes	3	01	No	No	3	01	Yes	No	3	
4/2*	23	No	No	3	-	No	No	3	-	Yes	No	3	

output definitions

Port	Configured DCB ports.
Loc-Adm Priorities	Indicates the priority for which PFC is enabled or disabled.
Loc-Adm MBC	Indicates if the local system is capable of bypassing MACsec processing when MACsec is disabled.
Loc-Adm Will	Indicates if the local system is willing to accept the PFC configuration of the remote system.
Loc-Adm Cap	Indicates the number of traffic classes on the local device that have simultaneously PFC enabled.
Loc-Oper Priorities	Indicates if PFC is enabled on the corresponding priority.
Loc-Oper MBC	Indicates if the local system is capable of bypassing MACsec processing when MACsec is disabled.

output definitions (continued)

Loc-Oper Will	Indicates if the local system is willing to accept the PFC configuration of the remote system.
Loc-Oper Cap	Indicates the number of traffic classes on the local device that have simultaneously PFC enabled.
Rem-Oper Priorities	Indicates if PFC is enabled on the corresponding priority on the remote system.
Rem-Oper MBC	Indicates if the remote system is capable of bypassing MACsec processing when MACsec is disabled.
Rem-Oper Will	Indicates if the remote system is willing to accept the PFC configuration of the local system.
Rem-Oper Cap	Indicates the number of traffic classes on the remote device that have simultaneously PFC enabled.

Release History

Release 7.3.1; command was introduced.

Related Commands

qos qsi dcb dcbx pfc Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis.

MIB Objects

```

lldpXdot1dcbxAdminPFCEnableTable
lldpXdot1dcbxAdminPFCBasicTable
lldpXdot1dcbxLocPFCEnableTable
lldpXdot1dcbxLocPFCBasicTable
lldpXdot1dcbxRemPFCEnableTable
lldpXdot1dcbxRemPFCBasicTable
  lldpV2LocPortIfIndex
  lldpXdot1dcbxAdminPFCEnableEnabled
  lldpXdot1dcbxAdminPFCMBC
  lldpXdot1dcbxAdminPFCWilling
  lldpXdot1dcbxAdminPFCCap
  lldpXdot1dcbxLocPFCEnableEnabled
  lldpXdot1dcbxLocPFCMBC
  lldpXdot1dcbxLocPFCWilling
  lldpXdot1dcbxLocPFCCap
  lldpXdot1dcbxRemPFCEnableEnabled
  lldpXdot1dcbxRemPFCMBC
  lldpXdot1dcbxRemPFCWilling
  lldpXdot1dcbxRemPFCCap

```

show qos pfc-lossless-usage

Displays the usage of the PFC lossless traffic class on the switch.

```
show qos pfc-lossless-usage
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays the PFC lossless traffic class usage on the switch.

Examples

```
-> show qos pfc-lossless-usage
Lossless Priorities in use      : 55,
Lossless Priorities reserved   : 60,
Lossless Priorities available  : 73
```

output definitions

Lossless Priorities in use	Indicates the number of PFC lossless priorities in use in the system.
Lossless Priorities reserved	Indicates the number of PFC lossless priorities in reserve in the system.
Lossless Priorities available	Indicates the number of priorities available to be configured as PFC lossless.

Release History

Release 7.3.1; command was introduced.

Related Commands

[qos qsi dcb dcbx pfc](#) Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis.

MIB Objects

```
alaDcbxConfig
  alaDcbxPfcLLPrioritiesUsed
  alaDcbxPfcLLPrioritiesReserved
  alaDcbxPfcLLPrioritiesAvailable
```

show qos qsi dcb pfc stats

Displays the traffic statistics per-port and per-traffic class.

show qos qsi [port slot/port[-port]] dcb pfc stats

Syntax Definitions

slot/port[-port]

A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use this command to view the PFC statistics.

Examples

```
-> show qos qsi port 1/1 dcb pfc stats
```

* displays packet count

Port	Q	PFC		PFC RX (ind)
		TC	TX (req)	
1/1	0	0	0	0
1/1	1	1	0	0
1/1	2	2	0	0
1/1	3	3	500	135
1/1	4	4	0	0
1/1	5	5	0	0
1/1	6	6	0	0
1/1	7	7	0	0

output definitions

Port	Configured DCB ports.
Q	The queue ID number.
TC	Indicates the traffic class to which the priority belongs.
Priority	Indicates the priority of the DCB port.
PFC TX (req)	Total count of PFC packets transmitted.
PFC RX (ind)	Total count of PFC packets received.

Release History

Release 7.3.1; command was introduced.

Related Commands

- | | |
|--|--|
| <code>qos qsi dcb dcbx pfc</code> | Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis. |
| <code>clear qos qsi dcb pfc stats</code> | Clears the port statistics. |

MIB Objects

```
alaDcbxPIPrioPriorityTable
  alaDcbxPIPrioIfIndex
  alaDcbxPIPrioTC
  alaDcbxPIPrioPriority
  alaDcbxPIPrioPFCPacketsTransmitted
  alaDcbxPIPrioPFCPacketsReceived
```

qos qsi stats admin-state

Enables the queue statistics collection on a port of DCB or Non-DCB profiles.

```
qos qsi {port chassis/slot/port[-port]} stats {admin-state {enable | disable} | interval minutes}
```

Syntax Definitions

<i>chassis/slot/port[-port]</i>	A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
stats admin-state enable	Enables the queue stats collection on the port.
stats admin-state disable	Disables the queue stats collection on the port.
<i>minutes</i>	Specifies the frequency at which the stats are updated. The valid range is 10–300 minutes.

Defaults

parameter	default
stats admin-state	disable
stats interval	60

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The queue stats collection must be enabled to start the collection on the port.

Examples

```
-> qos qsi port 1/5 stats admin-state enable
-> qos qsi port 1/5 stats interval 100
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsi stats	Displays the queue statistics for DCB and NDCB ports.
clear qos qsi dcb pfc stats	Clears the port statistics.

MIB Objects

```
alaVfcQsetInstanceTable  
  alaVfcQsetStatsAdmin  
  alaVfcQsetStatsInterval
```

show qos qsi stats

Displays the queue statistics for DCB and NDCB ports.

show qos qsi [port chassis/slot/port[-port]] stats [bytes] [packets]

Syntax Definitions

chassis/slot/port[-port] A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

bytes Displays the total number of bytes.

packets Displays the total number of packets.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The statistics is displayed only if the stats collection is enabled on the ports.

Examples

```
-> show qos qsi port 5/1 stats
```

* VOQ Total Drop doesn't account for queue aging

Port	Q	Tx	Total Drop
5/1	1	0	0
5/1	2	0	0
5/1	3	0	0
5/1	4	0	0
5/1	5	0	0
5/1	6	0	0
5/1	7	0	0
5/1	8	0	0

```
-> show qos qsi port 5/1 stats bytes
```

* VOQ Total Drop doesn't account for queue aging

Port	Q	Tx	Total Drop
5/1	1	0	0
5/1	2	0	0
5/1	3	0	0

5/1	4	0	0
5/1	5	0	0
5/1	6	0	0
5/1	7	0	0
5/1	8	0	0

output definitions

Port	Configured DCB ports.
Q	Number of packets or bytes in queue.
Total Tx	Displays the frequent at which statistics are updated. Specified in seconds.
Total Drop	Total packets or bytes dropped.

Release History

Release 7.3.1; command was introduced.

Related Commands

clear qos qsi dcb pfc stats Clears the port statistics.

MIB Objects

```
alaVfcQInstanceTable
  alaVfcQInstancePacketsEnqueued
  alaVfcQInstanceBytesEnqueued
  alaVfcQInstancePacketsDropped
  alaVfcQInstanceBytesDropped
```

clear qos qsi dcb pfc stats

Clears the queue statistics and DCB PFC stats.

clear qos qsi {port *slot/port*[-*port*]} dcb pfc stats

Syntax Definitions

slot/port[-*port*] A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the *slot/port* parameter to clear queue statistics associated with specific ports.
- Use the **dcb pfc** option to clear the DCB ports PFC statistics.

Examples

```
-> clear qos qsi port 1/2 stats
-> clear qos qsi port 2/1 dcb pfc stats
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show qos qsi stats](#) Displays the queue statistics for DCB and NDCB ports.

MIB Objects

```
alaVfcQsetInstanceTable
  alaVfcQsetStatsClear
```

29 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 43, “QoS Commands,”](#) for information about commands used to configure QoS software.

MIB information for the QoS policy commands is as follows:

Filename: alcatelIND1Qos.mib
Module ALCATEL-IND1-QoS-MIB

Important Note. Some of the commands listed here are not currently supported on one or more platforms. See command descriptions in this chapter and check release notes for information about commands that are not supported.

The QoS Policy commands are listed here:

Policy commands	policy rule policy validity-period policy list policy list rules policy condition policy action show policy action show policy condition show active policy rule show policy rule show policy validity period show active policy list show policy list
------------------------	---

Group commands	policy network group policy service policy service group policy mac group policy port group policy map group show policy network group show policy mac group show policy port group show policy map group show policy service show policy service group
Condition commands	policy condition policy condition source ip policy condition source ipv6 policy condition destination ipv6 policy condition multicast ip policy condition source network group policy condition destination network group policy condition multicast network group policy condition source ip-port policy condition destination ip-port policy condition source tcp-port policy condition destination tcp-port policy condition source udp-port policy condition destination udp-port policy condition ethertype policy condition established policy condition tcpflags policy condition service policy condition service group policy condition icmptype policy condition icmpcode policy condition ip-protocol policy condition ipv6 policy condition nh policy condition flow-label policy condition tos policy condition dscp policy condition source mac policy condition destination mac policy condition source mac group policy condition destination mac group policy condition source VLAN policy condition inner source-vlan policy condition destination vlan policy condition 802.1p policy condition inner 802.1p policy condition source port policy condition destination port policy condition source port group policy condition destination port group policy condition vrf policy condition fragments

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 cpu priority
policy action tos
policy action 802.1p
policy action dscp
policy action map
policy action permanent gateway-ip
policy action port-disable
policy action redirect port
policy action redirect linkagg
policy action no-cache
policy action mirror

Types of policies are generally determined by the kind of traffic they classify (policy conditions) and how the policy is enforced (policy actions). Commands used for particular types of policies are listed here. See the *OmniSwitch AOS Release 7 Network Configuration Guide* for more information about creating these types of policies and information about valid condition/action combinations.

Access Control Lists	policy condition policy action disposition policy rule
Traffic prioritization/shaping	policy action shared policy action priority policy action maximum bandwidth policy rule
802.1p/ToS/DSCP tagging or mapping	policy condition tos policy condition dscp policy condition 802.1p policy action tos policy action 802.1p policy action dscp policy action map policy rule
Network Address Translation (NAT)	policy condition source ip policy condition source ipv6 policy rule
Policy based port mirroring	policy action mirror
VLAN Stacking	policy condition inner source-vlan policy condition inner 802.1p

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] [save] [log [log-interval seconds]] [count {packets | bytes}] [trap] [default-list]
```

```
policy rule rule_name no {validity-period | save | log | trap | default-list}
```

```
no policy rule rule_name
```

Syntax Definitions

<i>rule_name</i>	The name of the policy rule, any alphanumeric string.
enable	Enables the policy rule.
disable	Disables the policy rule.
<i>precedence</i>	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.
<i>condition</i>	The condition name that is associated with this rule. Conditions are configured through the policy condition command.
<i>action</i>	The name of the action that is associated with this rule. Actions are configured through the policy action command.
<i>name</i>	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.
log	Configures the switch to log messages about specific flows coming into the switch that match this policy rule.
<i>seconds</i>	Configures how often to look for packets that match this policy rule when rule logging is applied (in the range from 0–3600 seconds). A value of 0 specifies to log as often as possible.
packets	Counts the number of packets that match the rule.
bytes	Counts the number of bytes that match the rule.
trap	Enables or disables traps for the rule.
default-list	Adds the rule to the QoS default policy list.

Defaults

parameter	default
enable disable	enable
<i>precedence</i>	0
log	no
<i>seconds</i>	60
packets bytes	packets
trap	enable
default-list	adds rule to the default list

Platforms Supported

OmniSwitch 10K, 6900

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 or to remove parameters from a particular rule. The change will not take effect, however, until the **qos apply** command is issued.
- 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.
- The **default-list** option adds the rule to the default policy list. Rules are added to this list by default when the rule is created. A rule can belong to multiple policy lists. As a result, the rule remains a member of the default list even when it is subsequently assigned to additional lists.
- If the rule is going to belong to a QoS policy list for a Universal Network Profile (UNP), use the **no default-list** option when creating the rule. Doing so will give the rule precedence over default list rules when the policy list is applied to UNP device traffic.

- Note that each time a rule is assigned to a policy list, an instance of that rule is created and each instance is allocated system resources. Use the **no default-list** option with this command to exclude the rule from the default policy list.
- If the **configuration snapshot** command is entered after the **policy rule** command is configured, the resulting ASCII file will include the following additional syntax for the **policy rule** command:

from {cli | ldap | blt}

This syntax indicates how the rule was created. The **cli** and **ldap** options 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 condition c2 action a2
-> policy rule rule3 condition c3 action a3 no default-list
-> policy rule rule2 precedence 65535
-> policy rule rule2 validity-period vp01
-> policy rule rule2 no precedence
-> policy rule rule2 no validity-period
-> policy rule rule3 no default-list
-> no policy rule rule2
```

Release History

Release 7.1.1; 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
- alaQoSRuleSave
- alaQoSRuleLog
- alaQoSRuleCountType
- alaQoSRulePacketCount
- alaQoSRuleByteCount
- alaQoSRuleDefaultList

alaQoSAppliedRuleTable

- alaQoSAppliedRuleName
- alaQoSAppliedRuleEnabled
- alaQoSAppliedRuleSource
- alaQoSAppliedRulePrecedence
- alaQoSAppliedRuleCondition
- alaQoSAppliedRuleAction
- alaQoSAppliedRuleSave
- alaQoSAppliedRuleLog
- alaQoSAppliedCountType
- alaQoSAppliedPacketCount
- alaQoSAppliedByteCount
- alaQoSAppliedDefaultList

policy validity-period

Configures a validity period that specifies the days and times in which a policy rule is in effect.

policy validity-period *name* [**days** *days*] [**months** *months*] [**hours** *hh:mm to hh:mm*] [**interval** *mm:dd:yyyy hh:mm to mm:dd:yyyy hh:mm*]

policy validity-period *name* **no** {**hours** / **interval**}

no policy validity-period *name*

Syntax Definitions

<i>name</i>	The name of the validity period (up to 31 alphanumeric characters).
<i>days</i>	The day(s) of the week this validity period is active. Enter the actual day of the week (e.g., monday , tuesday , wednesday , etc.).
<i>months</i>	The month(s) in which the validity period is active. Enter the actual month (e.g., january , february , march , etc.).
<i>hh:mm</i>	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).
<i>mm:dd:yyyy hh:mm</i>	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
<i>days</i>	no restriction
<i>months</i>	no restriction
<i>hh:mm</i>	no specific time
<i>mm:dd:yyyy hh:mm</i>	no interval

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show policy validity period	Displays information about policy validity periods.

MIB Objects

alaQoSValidityPeriodTable

- alaQoSValidityPeriodName
- alaQoSValidityPeriodSource
- alaQoSValidityPeriodDays
- alaQoSValidityPeriodDaysStatus
- alaQoSValidityPeriodMonths
- alaQoSValidityPeriodMonthsStatus
- alaQoSValidityPeriodHour
- alaQoSValidityPeriodHourStatus
- alaQoSValidityPeriodEndHour
- alaQoSValidityPeriodInterval
- alaQoSValidityPeriodIntervalStatus
- alaQoSValidityPeriodEndInterval

alaQoSAppliedValidityPeriodTable

- alaQoSAppliedValidityPeriodName
- alaQoSAppliedValidityPeriodSource
- alaQoSAppliedValidityPeriodDays
- alaQoSAppliedValidityPeriodDaysStatus
- alaQoSAppliedValidityPeriodMonths
- alaQoSAppliedValidityPeriodMonthsStatus
- alaQoSAppliedValidityPeriodHour
- alaQoSAppliedValidityPeriodHourStatus
- alaQoSAppliedValidityPeriodEndHour
- alaQoSAppliedValidityPeriodInterval
- alaQoSAppliedValidityPeriodIntervalStatus
- alaQoSAppliedValidityPeriodEndInterval

policy list

Configures a QoS policy list. There are two types of lists available: a Universal Network Profile (UNP) policy list and the default policy list. Rules assigned to a UNP list are applied to traffic classified into a specific profile. A default policy list is available when the switch boots up; all policy rules belong to this list unless otherwise specified.

policy list *list_name* **type unip** [**enable** | **disable**]

no policy list *list_name*

Syntax Definitions

<i>list_name</i>	The name to assign to the policy list. Note that the list name is case sensitive.
unip	Specifies the list type as a Universal Network Profile list.
enable	Enables the policy list.
disable	Disables the policy list.

Defaults

By default, the list is created as a UNP policy list. The **unip** parameter is optional.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove a policy list from the configuration.
- The default policy list available in every switch has no name and is not configurable. All QoS policy rules are assigned to the default list unless the **no default-list** option of the **policy rule** command is used at the time the rule is created.
- Once a policy list is created, use the **policy list rules** command to add rules to the list.
- 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 unip1 type unip
-> policy list unip1 disable
```



```
-> policy list unpl enable  
-> no policy list unpl
```

Release History

Release 7.2.1; command was introduced.

Related Commands

policy list rules	Assigns QoS policy rules to a QoS policy list.
policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show policy rule	Displays information for policy rules configured on the switch.
show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy list	Displays information for policy lists configured on the switch.

MIB Objects

```
alaQoSRuleGroupsTable  
  alaQoSRuleDefaultList  
  alaQoSRuleGroupsName  
  alaQoSRuleGroupsSource  
  alaQoSRuleGroupsType  
  alaQoSRuleGroupsEnabled  
  alaQoSRuleGroupsStatus  
alaQoSAppliedRuleGroupsTable  
  alaQoSAppliedRuleGroupsName  
  alaQoSAppliedRuleGroupsSource  
  alaQoSAppliedGroupsType  
  alaQoSAppliedGroupsEnabled  
  alaQoSAppliedRuleGroupsStatus
```

policy list rules

Assigns existing QoS policy rules to the specified QoS policy list.

policy list *list_name* **rules** *rule_name* [*rule_name2*...]

policy list *list_name* **no rules** *rule_name* [*rule_name2*...]

Syntax Definitions

<i>list_name</i>	The name of an existing QoS policy list. Note that the list name is case sensitive.
<i>rule_name</i>	The name of an existing QoS policy rule to include in the policy list.
<i>rule_name2</i>	Optional. The name of another QoS policy rule to include in the policy list. Separate each rule name specified with a space.

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 the default list unless the **no default-list** option of the **policy rule** command is used.

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Use the **no** form of the command to remove a policy rule from an existing list.
- The QoS policy list and rule names specified with this command must already exist in the switch configuration.
- This command is only used to assign rules to a UNP policy list. Create the rules for this type of list using the **no default-list** option of the **policy rule** command to ensure these rules take precedence over other default list rules when the UNP policy list is applied to device traffic.
- A rule may belong to a UNP list and the default 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 policy rule is disabled, then the rule is disabled for all lists even if a list to which the policy rule belongs is enabled.
- Any policy list configured through this command is not active on the switch until the **qos apply** command is issued.

Examples

```
-> policy list unpl rules r1 r2 r3
-> policy list unpl no rules r2
```

Release History

Release 7.2.1; command was introduced.

Related Commands

policy list	Configures a QoS policy list.
policy rule	Configures a policy rule on the switch and optionally associates that rule with a validity period.
show policy rule	Displays information for policy rules configured on the switch.
show active policy list	Displays only those policy lists that are currently being enforced on the switch.
show policy list	Displays information for policy lists configured on the switch.

MIB Objects

```
alaQoSRuleGroupsTable
  alaQoSRuleDefaultList
  alaQoSRuleGroupsName
  alaQoSRuleGroupsSource
  alaQoSRuleGroupsType
  alaQoSRuleGroupsEnabled
  alaQoSRuleGroupsStatus
alaQoSAppliedRuleGroupsTable
  alaQoSAppliedRuleGroupsName
  alaQoSAppliedRuleGroupsSource
  alaQoSAppliedGroupsType
  alaQoSAppliedGroupsEnabled
  alaQoSAppliedRuleGroupsStatus
```

policy network group

Configures a network group name and its associated IP addresses. The group 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

<i>net_group</i>	The name of the network group (up to 31 alphanumeric characters).
<i>ip_address</i>	An IPv4 address included in the network group. IPv6 addresses are not supported with network groups.
<i>net_mask</i>	The mask for the IPv4 address. If no mask is entered, the IPv4 address is assumed to be a host address.
<i>ip_address2</i>	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.
<i>net_mask2</i>	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 10K, 6900

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 7.1.1; 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

<i>service_group</i>	The name of the service group (up to 31 alphanumeric characters).
<i>service_name1</i>	The service name is configured through the policy service command and includes information about protocol, source port, and destination port.
<i>service_name2...</i>	Optional. Additional service names may be configured for a service group. Separate each service name with a space.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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. Then create a condition for this service group and a source port group, which can then be used in a deny rule. Refer to the switch *Network Configuration Guide* for more information about ACL security enhancements.
- If the **snapshot** command is entered after the **policy service group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service group** command:

from {cli | ldap | blt}

This syntax indicates how the service group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in service group, this setting is not configurable.

Examples

```
-> policy service group servgroup2 telnet ftp
-> policy service group servgroup2 no telnet
-> no policy service group servgroup2
```

Release History

Release 7.1.1; 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

<i>mac_group</i>	The name of the MAC group (up to 31 alphanumeric characters).
<i>mac_address</i>	The MAC address associated with the group (for example, 00:20:da:05:f6:23).
<i>mac_mask</i>	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.
<i>mac_address2</i>	Optional. Additional MAC addresses may be configured for a MAC group. Separate each address with a space.
<i>mac_mask2</i>	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 10K, 6900

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 7.1.1; 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

```
alaQoSACGroupsTable
  alaQoSACGroupsName
  alaQoSACGroupsSource
alaQoSAppliedMACGroupsTable
  alaQoSAppliedMACGroupsName
  alaQoSAppliedMACGroupsSource
alaQoSACGroupTable
  alaQoSACGroupMacAddr
  alaQoSACGroupMacMask
alaQoSAppliedMACGroupTable
  alaQoSAppliedMACGroupMacAddr
  alaQoSAppliedMACGroupMacMask
```

policy port group

Configures a port group and its associated slot and port numbers. A port group may be attached to a policy condition. The action associated with that policy will be applied to all members of the port group.

policy port group *group_name slot/port[-port] [slot/port[-port]...]*

no policy port group *group_name*

policy port group *group_name no slot/port[-port] [slot/port[-port]...]*

Syntax Definitions

<i>group_name</i>	The name of the port group (up to 31 alphanumeric characters).
<i>slot/port[-port]</i>	The slot and port (or port range) to be included in the group. At least one slot/port combination must be specified. Additional combinations may be included in the group; each combination should be separated by a space.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to configure a group of ports to which you want to apply QoS rules. Rather than create a condition for each port, group ports together. Use the **policy condition** command to associate a condition with the port group.
- Use the **no** form of the command to remove a port group from the configuration, or to remove a slot/port from a port group.
- If a range of ports is specified using the syntax *slot/port-port* (i.e., 2/1-8), a single port within that range cannot be removed on its own. The entire range must be deleted as it was entered.
- 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 10000 Network Configuration Guide* for more information about ACL security enhancements.
- Use the **qos user-port** command to configure the option to filter or administratively disable a port when a specific type of traffic (Spoof, RIP, BPDU, OSPF, and/or BGP) is received on a port that is a member of the pre-defined UserPorts group.

- If the **snapshot** command is entered after the **policy port group** command is configured, the resulting ASCII file will include the following additional syntax for the **policy port group** command:

from {cli | ldap | blt}

This syntax indicates how the port group was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

Examples

```
-> policy port group port_group4 3/1-2 4/3 5/4
-> policy port group port_group4 no 3/1-2
-> policy port group UserPorts 4/1-8 5/1-8
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Configures a policy condition. A port group may be configured as part of a policy condition.
qos apply	Applies configured QoS and policy settings to the current configuration.
policy action maximum bandwidth	Configures a maximum bandwidth value for a policy action.
show policy port group	Displays information about policy port groups.

MIB Objects

```
alaQoSPortGroupsTable
  alaQoSPortGroupsName
  alaQoSPortGroupsSource
alaQoSAppliedPortGroupsTable
  alaQoSAppliedPortGroupsName
  alaQoSAppliedPortGroupsSource
alaPortGroupTable
  alaQoSPortGroupSlot
  alaQoSPortGroupPort
  alaQoSPortGroupPortEnd
alaAppliedPortGroupTable
  alaQoSAppliedPortGroupSlot
  alaQoSAppliedPortGroupPort
  alaQoSAppliedPortGroupPortEnd
```

policy 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

<i>map_group</i>	The name of the map group (up to 31 alphanumeric characters).
<i>value1</i>	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).
<i>value2...</i>	The 802.1p, ToS, or DSCP value to be used in place of <i>value1</i> . Additional mapping pairs may be included.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>service_name</i>	The name of the service (up to 31 alphanumeric characters).
<i>protocol</i>	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 .
<i>port</i>	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 10K, 6900

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	<i>The protocol must be specified with at least one source or destination port.</i>
TCP ports for a service	source tcp port destination tcp port	<i>Keywords may be used in combination.</i>
UDP ports for a service	source udp port destination udp port	<i>Keywords may be used in combination.</i>

- 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 7.1.1; 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 | destination ip-port}
```

Syntax Definitions

<i>service_name</i>	The name of the service (up to 31 alphanumeric characters).
<i>protocol</i>	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.
<i>port</i>	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 10K, 6900

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 7.1.1; 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

<i>service_name</i>	The name of the service (up to 31 alphanumeric characters).
<i>port</i>	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 10K, 6900

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
-> policy service serv_5 no source tcp port
```

Release History

Release 7.1.1; 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

<i>service_name</i>	The name of the service (up to 31 alphanumeric characters).
<i>port</i>	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 10K, 6900

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
-> policy service service4 no destination tcp-port
```

Release History

Release 7.1.1; 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

<i>service_name</i>	The name of the service (up to 31 alphanumeric characters).
<i>port</i>	The well-known port number (or port range) for the desired UDP service. Specify a port range with a hyphen (for example, 22-23).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 source udp-port
```

Release History

Release 7.1.1; 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

<i>service_name</i>	The name of the service (up to 31 alphanumeric characters).
<i>port</i>	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 10K, 6900

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
-> policy service service4 no destination udp-port
```

Release History

Release 7.1.1; 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 your switch *Network Configuration Guide*.

policy condition *condition_name*

```
[source ip ip_address [mask netmask]]
[source ipv6 {any | ipv6_address [mask netmask]}]
[destination ip ip_address [mask netmask]]
[destination ipv6 {any | ipv6_address [mask netmask]}]
[multicast ip ip_address [mask netmask]]
[source network group network_group]
[destination network group network_group]
[multicast network group multicast_group]
[source ip port port[-port]]
[destination ip port port[-port]]
[source tcp port port[-port]]
[destination tcp port port[-port]]
[source udp port port[-port]]
[destination udp port port[-port]]
[ethertype etype]
[established]
[tcpflags {any | all} flag [mask flag]]
[service service]
[service group service_group]
[icmptype type]
[icmpcode code]
[ip protocol protocol]
[ipv6]
[nh next_header_value]
[flow-label flow_label_value]
[tos tos_value tos_mask]
[dscp {dscp_value[-value] [dscp_mask]}]
[source mac mac_address [mask mac_mask]]
[destination mac mac_address [mask mac_mask]]
[source mac group group_name]
[destination mac group mac_group]
[source vlan vlan_id]
[destination vlan vlan_id]
[802.1p 802.1p_value]
```

```
[source port slot/port[-port]]
[source port group group_name]
[destination port slot/port[-port]]
[destination port group group_name]
[vrf {vrf_name | default}]
[fragments]
```

```
no policy condition condition_name
```

Syntax Definitions

condition_name The name of the condition. Any alphanumeric string.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A policy condition and a policy action are combined to make a policy rule. See the [policy rule command on page 44-6](#).
- 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 7.1.1; 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
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionSource
```

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

<i>condition_name</i>	The name of the condition.
<i>ip_address</i>	The source IP address of the Layer 3 flow.
<i>netmask</i>	The mask for the source IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition.
any	Any source IPv6 address.
<i>ipv6_address</i>	A specific source IPv6 address.
<i>netmask</i>	The mask for the source IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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.

Examples

```
-> policy condition cond3 source ipv6 ::1234:531F:BCD2:F34A
```

Release History

Release 7.1.1; 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

<i>condition_name</i>	The name of the condition.
<i>ip_address</i>	The destination IP address of the Layer 3 flow.
<i>netmask</i>	The mask for the destination IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition.
any	Any destination IPv6 address.
<i>ipv6_address</i>	A specific destination IPv6 address.
<i>netmask</i>	The mask for the source IPv6 address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a destination IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- If a mask is not specified, the IPv6 address is assumed to be a host address.

Examples

```
-> policy condition cond3 destination ipv6 ::1234:531F:BCD2:F34A
```

Release History

Release 7.1.1; 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

<i>condition_name</i>	The name of the condition.
<i>ip_address</i>	The multicast IP address.
<i>netmask</i>	Optional. The mask for the multicast IP address.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition.
<i>network_group</i>	The name of the source network group. Network groups are configured through the policy network group command. See page 44-16 for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
policy network group	Configures a network group name and its associated IP addresses.
show policy condition	Shows information about policy conditions configured on the switch.
show policy network group	Displays information about policy network groups.

MIB Objects

alaQoSConditionTable

 alaQoSConditionName

 alaQoSConditionSourceNetworkGroup

alaQoSAppliedConditionTable

 alaQoSAppliedConditionName

 alaQoSAppliedConditionSourceNetworkGroup

policy condition destination network group

Associates a destination network group with a policy condition.

policy condition *condition_name* **destination network group** *network_group*

policy condition *condition_name* **no destination network group**

Syntax Definitions

condition_name

The name of the condition.

network_group

The name of the destination network group. Network groups are configured through the **policy network group** command. See [page 44-16](#) for more information about this command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

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 7.1.1; 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 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition.
<i>port</i>	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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

gos 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

<i>condition_name</i>	The name of the condition.
<i>port</i>	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 10K, 6900

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 7.1.1; 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
  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

<i>condition_name</i>	The name of the condition.
<i>port</i>	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 10K, 6900

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 7.1.1; 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
  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

<i>condition_name</i>	The name of the condition.
<i>port</i>	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 10K, 6900

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 7.1.1; 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
  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

<i>condition_name</i>	The name of the condition.
<i>port</i>	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 10K, 6900

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 udp-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 7.1.1; 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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable

 alaQoSConditionName

 alaQoSConditionEthertype

 alaQoSConditionEthertypeStatus

alaQoSAppliedConditionTable

 alaQoSAppliedConditionName

 alaQoSAppliedConditionEthertype

 alaQoSAppliedConditionEthertypeStatus

policy condition established

Configures an established TCP connection as a policy condition. A connection is considered established if the **ack** or **rst** flags in the TCP header of the packet are set.

policy condition *condition_name* **established**

policy condition *condition_name* **no established**

Syntax Definitions

condition_name The name of the condition.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove **established** from a condition; however, at least one classification parameter must be associated with a condition.
- When an initial TCP connection packet is received only the **syn** flag is set. As a result, TCP packets are only examined if they are not the starting packet.
- Typically this condition is used in combination with **source ip**, **destination ip**, **source port**, **destination port**, **source TCP port**, or **destination TCP port** conditions.
- 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 7.1.1; 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

<i>condition_name</i>	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). <i>The E and W flags are currently not supported.</i>

Defaults

parameter	default
any all	all

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove **tcpflags** from a condition; however, at least one classification parameter must be associated with a condition.
- Use the **any** option to indicate that a match on any one of the specified TCP flags qualifies as a match for the condition. Use the **all** option to indicate that a match on all specified TCP flags is required to qualify as a match for the condition.
- Enter one or more TCP flags after the **any** or **all** keyword to indicate that the value of the flag bit must be set to one to qualify as a match.
- Enter one or more TCP flags after the **mask** keyword to indicate which TCP flags to match.
- If a TCP flag is specified as part of the **mask** but does not have a corresponding match value specified with the **any** or **all** options, then zero is assumed as the match value. For example, **tcpflags all f s mask f s a** looks for the following bit values to determine a match: **f**=1, **s**=1, **a**=0.
- Typically this condition is used in combination with **source ip**, **destination ip**, **source port**, **destination port**, **source TCP port**, or **destination TCP port** conditions.
- 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 7.1.1; 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 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition.
<i>service_group</i>	The service group name. Service groups are configured through the policy service group command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 global QoS and policy settings to the current configuration (changes will be active and stored in flash).
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable

 alaQoSConditionName

 alaQoSConditionServiceGroup

alaQoSAppliedConditionTable

 alaQoSAppliedConditionName

 alaQoSAppliedConditionServiceGroup

policy condition icmp-type

Configures an ICMP type value to use for traffic classification.

policy condition *condition_name* **icmp-type** *type*

policy condition *condition_name* **no icmp-type**

Syntax Definitions

<i>condition_name</i>	The name of the condition.
<i>type</i>	The ICMP type value, in the range 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 icmp-type 100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition icmp-code	Configures an ICMP code value for traffic classification.
policy condition	Creates a policy condition.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
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

<i>condition_name</i>	The name of the condition.
<i>code</i>	The ICMP code value, in the range 0–255.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

policy condition icmptype	Configures an ICMP type value for traffic classification.
policy condition	Creates a policy condition.
qos apply	Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
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
<i>protocol</i>	6

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 global QoS and policy settings to the current configuration (changes will be active and stored in flash).

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 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove IPv6 traffic as a condition; however, at least one classification parameter must be associated with a condition.
- When the **ipv6** keyword is used in a condition, a policy that uses the condition is considered an IPv6 policy. IPv6 policies are effected only on IPv6 traffic. All other IP policies are considered IPv4 policies and are effected only on IPv4 traffic.
- IPv6 Layer 4 policies are supported and are configured using the **ipv6** keyword in a condition that specifies Layer 4 information, services, or service groups. Note that IPv6 Layer 4 policies only work with packets that contain a single header.
- The **icmptype** and **icmpcode** keywords in an IPv6 policy imply the ICMPv6 protocol, not the ICMPv4 protocol.

Examples

```
-> policy condition cond4 ipv6
-> policy condition cond5 ipv6 tos 7
-> policy condition cond6 ipv6 source port 1/1
-> policy condition cond7 ipv6 source tcp port 21
-> policy condition cond8 ipv6 source tcp port 0-1024
-> policy condition cond6 no ipv6
```

Release History

Release 7.1.1; 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 nh

Configures an IPv6 next header value as a policy condition. This value is compared to the next header value in the IPv6 header.

policy condition *condition_name* **nh** *next_header_value*

policy condition *condition_name* **no nh**

Syntax Definitions

condition_name The name of the condition.

next_header_value The next header value (0–255).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of the command to remove the next header value as a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 nh 100
-> policy condition cond4 no nh
```

Release History

Release 7.1.1; 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
  alaQoSConditionIpv6NH
  alaQoSConditionIpv6NHStatus
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionIpv6NH
  alaQoSAppliedConditionIpv6NHStatus
```

policy condition flow-label

Configures an IPv6 flow label value as a policy condition. This value is compared to the flow label value in the IPv6 header.

policy condition *condition_name* **flow-label** *flow_label_value*

policy condition *condition_name* **no flow-label**

Syntax Definitions

<i>condition_name</i>	The name of the condition.
<i>flow_label_value</i>	The flow-label value (0–1048575).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of the command to remove the flow label value as a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond4 flow-label 1500
-> policy condition cond4 no flow-label
```

Release History

Release 7.1.1; 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

 alaQoSConditionIpv6FlowLabel

 alaQoSConditionIpv6FlowLabelStatus

alaQoSAppliedConditionTable

 alaQoSAppliedConditionName

 alaQoSAppliedConditionIpv6FlowLabel

 alaQoSAppliedConditionIpv6FlowLabelStatus

policy condition tos

Configures the precedence bits in the Type of Service (ToS) byte value for a policy condition.

policy condition *condition_name* **tos** *tos_value* [**mask** *tos_mask*]

policy condition *conditioning* **no tos**

Syntax Definitions

<i>conditioning</i>	The name of the condition. May be an existing condition name or a new condition.
<i>tos_value</i>	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).
<i>tos_mask</i>	The mask for the ToS bits, in the range 0–7.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
{ <i>dscp_value</i> [- <i>value</i>]}	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).
<i>dscp_mask</i>	The mask for the DiffServ Code Point, in the range 0–63.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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.
- When a DSCP policy condition is configured on one of these switches, QoS automatically calculates the appropriate mask value.

Examples

```
-> policy condition cond4 dscp 10
-> policy condition cond5 dscp 20-30
```

Release History

Release 7.1.1; 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

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>mac_address</i>	The source MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23)
<i>mac_mask</i>	Optional. The mask for the source MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>mac_address</i>	The destination MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23).
<i>mac_mask</i>	Optional. The mask for the destination MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>group_name</i>	The name of the source MAC group, configured through the policy mac group command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>mac_group</i>	The name of the destination MAC group, configured through the policy mac group command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

Use the **no** form of the command to remove a source VLAN from a policy condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond5 source vlan 3
```

Release History

Release 7.1.1; 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 inner source-vlan

Configures an inner source VLAN ID as a policy condition. This condition applies to double-tagged VLAN Stacking traffic and is used to classify such traffic based on the inner VLAN ID tag, also known as the customer VLAN ID.

policy condition *condition_name* **inner source-vlan** *vlan_id*

policy condition *condition_name* **no inner source-vlan**

Syntax Definitions

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>vlan_id</i>	The inner source VLAN ID (customer VLAN ID) to match on double-tagged packets.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove an inner source VLAN from a policy condition; however, at least one classification parameter must be associated with a condition.
- Policies that use the inner source VLAN condition are referred to as QoS VLAN Stacking policies. These are separate policies from those configured through the VLAN Stacking Service application.

Examples

```
-> policy condition cond5 inner source-vlan 3
-> policy condition cond5 no inner source-vlan
```

Release History

Release 7.1.1; 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

 alaQoSConditionInnerSourceVlan

 alaQoSConditionInnerSourceVlanStatus

alaQoSAppliedConditionTable

 alaQoSAppliedConditionName

 alaQoSAppliedConditionInnerSourceVlan

 alaQoSAppliedConditionInnerSourceVlanStatus

policy condition destination vlan

Configures a destination VLAN (multicast only) for a policy condition. Use the **no** form of the command to remove a destination VLAN from a condition.

policy condition *condition_name* **destination vlan** *vlan_id*

policy condition *condition_name* **no destination vlan**

Syntax Definitions

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>vlan_id</i>	The destination VLAN ID for the flow.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable

 alaQoSConditionName

 alaQoSConditionDestinationVlan

alaQoSAppliedConditionTable

 alaQoSAppliedConditionName

 alaQoSAppliedConditionDestinationVlan

policy condition 802.1p

Configures the 802.1p value for a policy condition.

policy condition *condition_name* **802.1p** *802.1p_value*

policy condition *condition_name* **no 802.1p**

Syntax Definitions

condition_name The name of the condition. May be an existing condition name or a new condition.

802.1p_value The 802.1p value in the 802.1Q VLAN tag for the flow. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of the command to remove an 802.1p value for a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond3 802.1p 7
```

Release History

Release 7.1.1; 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  
  alaQoSCondition8021p  
alaQoSAppliedConditionTable  
  alaQoSAppliedConditionName  
  alaQoSAppliedCondition8021p
```

policy condition inner 802.1p

Configures an inner (customer) source 802.1p value for a policy condition. This condition applies to double-tagged VLAN Stacking traffic and is used to classify such traffic based on the inner 802.1p bit value.

policy condition *condition_name* **inner 802.1p** *802.1p_value*

policy condition *condition_name* **no inner 802.1p**

Syntax Definitions

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>802.1p_value</i>	The inner 802.1p value of the inner 802.1Q VLAN tag (customer VLAN) to match on double-tagged packets. Values range from 0 (lowest priority) to 7 (highest priority).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove an 802.1p value for a condition; however, at least one classification parameter must be associated with a condition.
- Policies that use the inner 802.1p condition are referred to as QoS VLAN Stacking policies. These are separate policies from those configured through the VLAN Stacking Service application.

Examples

```
-> policy condition cond3 inner 802.1p 7
-> policy condition cond3 no inner 802.1p
```

Release History

Release 7.1.1; 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
  alaQoSConditionInner8021p
  alaQoSConditionInner8021pStatus
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionInner8021p
  alaQoSAppliedConditionInner8021pStatus
```

policy condition source port

Configures a source port number for a policy condition. Use the **no** form of the command to remove a source port number from a condition.

policy condition *condition_name* **source port** *slot/port[-port]*

policy condition *condition_name* **no source port**

Syntax Definitions

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>slot/port</i>	The slot and port number (or range of ports) on which the frame is received.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of the command to remove a source port from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond2 source port 3/1
-> policy condition cond3 source port 3/2-4
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy condition	Creates a policy condition.
show policy condition	Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable

 alaQoSConditionName

 alaQoSConditionSourceSlot

 alaQoSConditionSourcePort

 alaQoSConditionSourcePortEnd

alaQoSAppliedConditionTable

 alaQoSAppliedConditionName

 alaQoSAppliedConditionSourceSlot

 alaQoSAppliedConditionSourcePort

 alaQoSAppliedConditionSourcePortEnd

policy condition destination port

Configures a destination port number for a policy condition.

policy condition *condition_name* **destination port** *slot/port[-port]*

policy condition *condition_name* **no destination port**

Syntax Definitions

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>slot/port</i>	The slot and port number (or range of ports) on which the frame is received.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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
-> policy condition cond4 destination port 4/3-4
```

Release History

Release 7.1.1; 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

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>group_name</i>	The name of the source port group. Port groups are configured through the policy port group command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of the command to remove a source port group from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond6 source port group portgr4
```

Release History

Release 7.1.1; 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. Use the **no** form of the command to remove a destination port group from a condition.

policy condition *condition_name* **destination port group** *group_name*

policy condition *condition_name* **no destination port**

Syntax Definitions

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>group_name</i>	The name of the destination port group. Port groups are configured through the policy port group command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of the command to remove a destination port group from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond6 destination port group portgr4
```

Release History

Release 7.1.1; 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

 alaQoSConditionDestinationPortGroup

alaQoSAppliedConditionTable

 alaQoSAppliedConditionName

 alaQoSAppliedConditionDestinationPortGroup

policy condition vrf

Associates a Virtual Routing and Forwarding (VRF) instance with a policy condition.

policy condition *condition_name* **vrf** {*vrf_name* / **default**}

policy condition *condition_name* **no vrf**

Syntax Definitions

<i>condition_name</i>	The name of the condition. May be an existing condition name or a new condition.
<i>vrf_name</i>	The name of the VRF instance to which the QoS policy condition applies.
default	Specifies the default VRF instance.

Defaults

By default, QoS policy conditions are not associated with any VRF instance. The policy applies across all instances.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove a VRF instance from a condition; however, at least one classification parameter must be associated with a condition.
- VRF policies are configured in the default VRF, similar to how all other QoS policies are configured. If the VRF name specified does not exist, the policy is not allocated any system resources.
- Policies that do not specify a VRF name are considered global policies and are applied across all VRF instances and VLANs.
- Policies that specify the default VRF apply only to traffic in the default VRF instance.
- Policies that specify a VRF name apply only to traffic in the VRF instance associated with that name.
- The **switch** network group is supported only in VRF policies that specify the default VRF instance. If this group is specified in a global policy (no VRF specified) then the policy is applied across all VRF instances.

Examples

```
-> policy condition cond6 vrf engr-vrf
-> policy condition cond7 vrf default
-> policy condition cond6 no vrf
```

Release History

Release 7.1.1; 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
  alaQoSConditionVrfName
  alaQoSConditionVrfNameStatus
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionVrfName
  alaQoSAppliedConditionVrfNameStatus
```

policy condition fragments

Associates TCP packet fragments with a policy condition.

policy condition *condition_name* **fragments**

policy condition *condition_name* **no fragments**

Syntax Definitions

condition_name The name of the condition. May be an existing condition name or a new condition.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove TCP packet fragments from a condition; however, at least one classification parameter must be associated with a condition.

Examples

```
-> policy condition cond6 fragments
-> policy condition cond7 no fragments
```

Release History

Release 7.1.1; 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
  alaQoSConditionFragments
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionFragments
```

policy action

Configures or deletes a QoS action. A QoS action describes how traffic that matches a particular QoS condition should be treated. It may specify a particular set of bandwidth and queue parameters, or it may simply specify whether the flow is allowed or denied on the switch.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the **no** form for keywords to remove the parameter from the action.

Note that some action parameters may not be supported depending on the platform you are using. Also some action parameters may not be supported with some conditions. See the condition table in your switch's *Network Configuration Guide*.

policy action *action_name*

[**disposition** {**accept** | **drop** | **deny**}]
 [**shared**]
 [**priority** *priority_value*]
 [**maximum bandwidth** *bps*]
 [**maximum depth** *bytes*]
 [**cir** *bps* [**cbs** *bps*] [**pir** *bps*] [**pbs** *bps*] [**cpu priority** *priority*] [**color-only**]
 [**tos** *tos_value*]
 [**802.1p** *802.1p_value*]
 [**dscp** *dscp_value*]
 [**map** {**802.1p** | **tos** | **dscp**} **to** {**802.1p** | **tos** | **dscp**} **using** *map_group*]
 [**permanent gateway ip** *ip_address*]
 [**port-disable**]
 [**redirect port** *slot/port*]
 [**redirect linkagg** *link_agg*]
 [**no-cache**]
 [{**ingress** | **egress** | **ingress egress** | **no**} **mirror** *slot/port*]

policy no action *action_name*

Syntax Definitions

action_name A name for the action, any alphanumeric string.

Defaults

By default, no drop algorithm is configured for the action, and any queues created by the action are not shared.

parameter	default
accept drop deny	accept

Platforms Supported

OmniSwitch 10K, 6900

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 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.
- If the **snapshot** command is entered after the **policy action** command is configured, the resulting ASCII file will include the following additional syntax for the **policy action** command:

from {cli | ldap | blt}

This syntax indicates how the action was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in action, this setting is not configurable.

Examples

```
-> policy action action1 accept
```

Release History

Release 7.1.1; command was introduced.

Related Commands

policy condition	Configures a condition associated with the action.
qos apply	Applies configured QoS and policy settings to the current configuration.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable  
  alaQoSActionName  
  alaQoSActionSource  
alaQoSAppliedActionTable  
  alaQoSAppliedActionName  
  alaQoSAppliedActionSource
```

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

<i>action_name</i>	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 10K, 6900

Usage Guidelines

Use the **no** form of this command to remove a disposition from an action.

Examples

```
-> policy action a3 disposition deny
-> policy action a3 no disposition
```

Release History

Release 7.1.1; 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 bandwidth sharing among multiple QoS rules that use the same maximum bandwidth action.

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 10K, 6900

Usage Guidelines

- If the **shared** policy action is not specified, then each bandwidth rule will implement a separate instance of the specified bandwidth allocation.
- Use the **no** form of the command to disable sharing.

Example

```
-> policy action action5 maximum bandwidth 10m shared
-> policy action action6 maximum bandwidth 10m shared
-> policy action action5 no shared
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action maximum bandwidth	Creates a maximum bandwidth policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
  alaQoSActionName
  alaQoSActionShared
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionShared
```

policy action priority

Configures the priority for queuing a flow to which the QoS action applies.

policy action *action_name* **priority** *priority_value*

policy action *action_name* **no priority**

Syntax Definitions

action_name

The name of the action.

priority_value

The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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.

Examples

```
-> policy action action1 priority 1
-> policy action action1 no priority
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[qos apply](#)

Applies configured QoS and policy settings to the current configuration.

[policy action](#)

Creates a policy action.

[show policy action](#)

Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
  alaQoSActionName
  alaQoSActionPriority
  alaQoSActionPriorityStatus
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionPriority
  alaQoSAppliedActionPriorityStatus
```

policy action maximum bandwidth

Configures a maximum bandwidth value for a policy action.

policy action *action_name* **maximum bandwidth** *bps[k | m | g | t]*

policy action *action_name* **no maximum bandwidth**

Syntax Definitions

<i>action_name</i>	The name of the action.
<i>bps[k m g t]</i>	The maximum amount of bandwidth, in bits-per-second, for all traffic that ingresses on the port. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k , 5m , 1g , 1t).

Defaults

parameter	default
<i>k m g t</i>	k

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove a maximum bandwidth value from an action.
- If the maximum bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number **10** is specified, **10K** is the maximum bandwidth value used. However, if **10G** is specified, the maximum bandwidth value applied is **10** gbps.
- Use the **shared** policy action to enabling sharing of bandwidth across policy rules that specify the same maximum bandwidth action.

Examples

```
-> policy action action3 maximum bandwidth 10000
-> policy action action4 maximum bandwidth 10k shared
-> policy action action5 maximum bandwidth 10k shared
-> policy action action4 no maximum bandwidth
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
  alaQoSActionName
  alaQoSActionMaximumBandwidth
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionMaximumBandwidth
```

policy action maximum depth

Configures the maximum bucket size assigned to this action. The bucket size determines how much the traffic can burst over the maximum bandwidth rate. When the bucket size is reached, the switch starts to drop packets.

policy action *action_name* **maximum depth** *bps*[**k** | **m** | **g** | **t**]

policy action *action_name* **no maximum depth**

Syntax Definitions

<i>action_name</i>	The name of the action.
<i>bps</i> [k m g t]	The maximum bucket size, in bits-per-second. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k , 5m , 1g).

Defaults

parameter	default
k m g t	k

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a maximum depth value from a policy action.
- If the maximum depth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number **10** is specified, **10K** is the maximum depth value used. However, if **10G** is specified, the maximum depth value applied is **10** gbps.
- A maximum depth action is used in combination with a maximum bandwidth action.

Examples

```
-> policy action action2 maximum depth 100
-> policy action action2 no maximum depth
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

```
alaQoSActionTable
  alaQoSActionName
  alaQoSActionMaximumDepth
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionMaximumDepth
```

policy action cir

Configures a Tri-Color Marking (TCM) policy action. This type of action includes parameters for Committed Information Rate (CIR), Committed Burst Size (CBS), Peak Information Rate (PIR), and Peak Burst Size (PBS). The TCM policier meters and marks packets red, green, or yellow based on the parameter values of this policy action.

policy action *action_name* **cir** *bps* [*cbs bps*] [*pir bps*] [*pbs bps*] [**color-only**]

policy action *action_name* **no cir**

policy action *action_name* **no pir**

Syntax Definitions

<i>action_name</i>	The name of the action.
<i>bps</i> [k m g t]	The maximum amount of bandwidth, in bits-per-second, for all traffic that ingresses on the port. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k , 5m , 1g , 1t).
color-only	Disables TCM rate limiting based on the metering results. Packets are only marked the specific color that applies to the level of packet conformance.

Defaults

parameter	default
cbs pir pbs <i>bps</i>	0
k m g t	k
<i>priority</i>	0

By default, this action enables rate limiting based on TCM marking and metering.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the TCM parameter values.
- If the **color-only** parameter is specified with this command, the TCM action will only mark packet color; packets are not rate limited based on the metering results. In this case, packets are then subject to any rate limiting specifications as defined in the queue management configuration for the switch. See the [qos qsi wred](#) command for more information.
- This implementation of TCM supports two rate limiting modes: Single-Rate (srTCM) and Two-Rate (trTCM). The srTCM mode marks packets based only on the CIR and the two burst sizes: CBS and PBS. The trTCM mode marks packets based on both the CIR and PIR and their associated CBS and PBS values.

- There is no explicit CLI command to configure the mode (srTCM or trTCM) in which the TCM meter operates. Instead, the mode is determined by the CIR and PIR values configured for the policy action. If the PIR value is greater than the CIR value, trTCM is used. If the PIR value is less than the CIR value, srTCM is used.
- Configuring CIR and CBS is similar to configuring a maximum bandwidth. Configuring CIR and PIR is similar to configuring maximum depth.
- The number of packets counted as a result of the counter color mode setting is displayed using the **show active policy rule** command. These statistics are only shown for those rules that are configured with a TCM policy action.

Examples

The following command examples configure srTCM (the default):

```
-> policy action A3 cir 10M
-> policy action A4 cir 10M cbs 4k
-> policy action A5 cir 10M cbs 4k pir 10M
-> policy action A6 cir 10M cbs 4k pir 10M pbs 4k
-> policy action a7 cir 5M cbs 2k color-only
-> policy action A3 no cir
-> policy action A5 no pir
```

The following command examples configure trTCM (note that PIR is greater than CIR):

```
-> policy action A7 cir 10M cbs 4k pir 20M
-> policy action A8 cir 10M cbs 4k pir 20M pbs 40M
-> policy action a9 cir 5M cbs 1M pbs 10M pbs 2M color-only
-> policy action A7 no cir
```

Release History

Release 7.1.1; 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
  alaQoSActionCIR
  alaQoSActionCIRStatus
  alaQoSActionCBS
  alaQoSActionCBSStatus
  alaQoSActionPIR
  alaQoSActionPIRStatus
  alaQoSActionPBS
  alaQoSActionPBSStatus
  alaQoSActionColorOnly
alaQoSAppliedActionTable
  alaQoSAppliedActionCIR
  alaQoSAppliedActionCIRStatus
```

```
alaQoSAppliedActionCBS  
alaQoSAppliedActionCBSStatus  
alaQoSAppliedActionPIR  
alaQoSAppliedActionPIRStatus  
alaQoSAppliedActionPBS  
alaQoSAppliedActionPBSStatus  
alaQoSAppliedColorOnly
```

policy action cpu priority

Configures a CPU priority policy action.

policy action *action_name* **cpu priority** *priority*

policy action *action_name* **no cpu priority**

Syntax Definitions

<i>action_name</i>	The name of the action.
<i>priority</i>	The CPU queue on which packets destined for the CPU are received. The valid range is 0–31.

Defaults

By default, the CPU priority is set to zero.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to remove the CPU priority parameter value.

Examples

```
-> policy action A7 cpu priority 15
-> policy action A8 cpu priority 31
-> policy action A7 no cpu priority
```

Release History

Release 7.1.1; 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
  alaQoSActionCPUPriority
  alaQoSActionCPUPriorityStatus
alaQoSAppliedActionTable
  alaQoSAppliedActionCPUPriority
  alaQoSAppliedActionCPUPriorityStatus
```

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

<i>action_name</i>	The name of the action.
<i>tos_value</i>	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 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a ToS value from a policy action.
- Note that specifying both ToS and DSCP in the same action is *not* allowed.

Examples

```
-> policy action action3 tos 4  
-> policy action action3 no tos
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

alaQoSActionTable

 alaQoSActionName

 alaQoSActionTos

alaQoSAppliedActionTable

 alaQoSAppliedActionName

 alaQoSAppliedActionTos

policy action 802.1p

Configures a value to be set in the 802.1p bits of the 802.1Q byte of an outgoing frame for traffic that matches a policy with this action.

policy action *action_name* **802.1p** *802.1p_value*

policy action *action_name* **no 802.1p**

Syntax Definitions

<i>action_name</i>	The name of the action.
<i>802.1p_value</i>	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 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove an 802.1p value from a policy action.
- Note that specifying both ToS and DSCP in the same action is not allowed.

Examples

```
-> policy action action4 802.1p 7
-> policy action action4 no 802.1p
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

alaQoSActionTable

 alaQoSActionName
 alaQoSAction8021p

alaQoSAppliedActionTable

 alaQoSAppliedActionName
 alaQoSAppliedAction8021p

policy action dscp

Configures a Differentiated Services Code Point (DSCP) value to be set in an outgoing flow for traffic that matches rules with this action.

policy action *action_name* **dscp** *dscp_value*

policy action *action_name* **no dscp**

Syntax Definitions

<i>action_name</i>	The name of the action.
<i>dscp_value</i>	The DSCP value to be set, in the range 0–63.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a DSCP value from a policy action.
- Note that specifying both ToS and DSCP in the same action is *not* allowed.

Examples

```
-> policy action action2 dscp 61
-> policy action action2 no dscp
```

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply	Applies configured QoS and policy settings to the current configuration.
policy action	Creates a policy action.
show policy action	Displays information about policy actions.

MIB Objects

alaQoSActionTable

alaQoSActionName

alaQoSActionDscp

alaQoSAppliedActionTable

alaQoSAppliedActionName

 alaQoSAppliedActionDscp

policy action map

Configures a mapping group for a policy action.

policy action map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group*

policy action no map

Syntax Definitions

802.1p	Indicates that an 802.1p value should be mapped.
tos	Indicates that a ToS value should be mapped.
dscp	Indicates that a DSCP value should be mapped.
<i>map_group</i>	The name of the map group, configured through the policy map group command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 determine the outgoing 802.1p and ToS based on whether or not the port is trusted or untrusted).

- 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 7.1.1; 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 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove a gateway IP address from a policy action.
- If the gateway goes down, the traffic to be routed over the gateway will be dropped.

Examples

```
-> policy action pbr2 permanent gateway-ip 10.10.2.1  
-> policy action pbr2 no permanent gateway-ip
```

Release History

Release 7.1.1; 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

 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 10K, 6900

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** or **clear violation** command to administratively enable the port, or physically disconnect and reconnect the port cable.

Examples

```
-> policy action pd01 port-disable  
-> policy action pb02 no port-disable
```

Release History

Release 7.1.1; 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.
interfaces	Administratively enables or disables a port.
clear violation	Administratively clears the violation that disabled the port or link aggregate and restores the port to enabled status.

MIB Objects`alaQoSActionTable``alaQoSActionName``alaQoSActionPortdisable``alaQoSAppliedActionTable``alaQoSAppliedActionName``alaQoSAppliedActionPortdisable`

policy action redirect port

Redirects all traffic (flooded, bridged, routed, and multicast) matching a redirect policy to the specified port instead of the port to which the traffic was destined.

policy action *action_name* **redirect port** *slot/port*

policy action *action_name* **no redirect port**

Syntax Definitions

action_name The name of the action.

slot/port The slot and port number that will receive the redirected traffic.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove **redirect port** from the policy action.
- When redirecting routed traffic from VLAN A to VLAN B, the redirect port must belong to VLAN B (tagged or default VLAN).
- Routed packets (from VLAN A to VLAN B) are not modified after they are redirected; the source and MAC address remain the same. In addition, if the redirect port is tagged, the redirected packets will have a tag from the ingress VLAN A.
- If a route exists for the redirected flow, then redirected packets are the final post-routing packets.
- If a route does not exist for the redirected flow, the flow is not redirected to the specified port or link aggregate and is “blackholed”. As soon as a route is available, the flow is then redirected as specified in the policy.
- In most cases, a redirected flow will *not* trigger an update to the routing and ARP tables. If necessary, create a static route for the flow or assign the redirect port to the ingress VLAN (VLAN A) to send packets to the redirect port until a route is available.
- When redirecting bridged traffic on VLAN A, the redirect port must belong to VLAN A (tagged or default VLAN).

Examples

```
-> policy action rp01 redirect port 1/12
-> policy action rp01 no redirect port
```

Release History

Release 7.1.1; 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
  alaQoSActionRedirectSlot
  alaQoSActionRedirectPort
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionRedirectSlot
  alaQoSAppliedActionRedirectPort
```

policy action redirect linkagg

Redirects all traffic (flooded, bridged, routed, and multicast) matching a redirect policy to the specified link aggregate ID instead of the link aggregate to which the traffic was destined.

policy action *action_name* **redirect linkagg** *link_agg*

policy action *action_name* **no redirect linkagg**

Syntax Definitions

action_name The name of the action.

link_agg The link aggregate ID number (0–32) to assign to the specified VLAN. See [Chapter 12, “Link Aggregation Commands.”](#)

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove **redirect linkagg** from the policy action.
- When redirecting routed traffic from VLAN A to VLAN B, the redirect link aggregate ID must belong to VLAN B (tagged or default VLAN).
- Routed packets (from VLAN A to VLAN B) are not modified after they are redirected; the source and MAC address remain the same. In addition, if the redirect link aggregate ID is tagged, the redirected packets will have a tag from the ingress VLAN A.
- If a route exists for the redirected flow, then redirected packets are the final post-routing packets.
- If a route does not exist for the redirected flow, the flow is not redirected to the specified link aggregate ID and is “blackholed”. As soon as a route is available, the flow is then redirected as specified in the policy.
- In most cases, a redirected flow will *not* trigger an update to the routing and ARP tables. If necessary, create a static route for the flow or assign the redirect port or link aggregate ID to the ingress VLAN (VLAN A) to send packets to the redirect port until a route is available.
- When redirecting bridged traffic on VLAN A, the redirect port or link aggregate ID must belong to VLAN A (tagged or default VLAN).

Examples

```
-> policy action rp01 redirect port 1/12
-> policy action rp01 no redirect port
```

Release History

Release 7.1.1; 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
  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 10K, 6900

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 7.1.1; 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  
    alaQoSActionNocache  
alaQoSAppliedActionTable  
    alaQoSAppliedActionName  
    alaQoSAppliedActionNocache
```

policy action mirror

Mirrors ingress, egress, or both ingress and egress packets that match a mirroring policy to the specified port.

policy action *action_name* [**ingress** | **egress** | **ingress egress**] **mirror** *slot/port*

policy action *action_name* **no mirror** *slot/port*

Syntax Definitions

<i>action_name</i>	The name of the action.
ingress	Mirrors ingress packets.
egress	Mirrors egress packets.
ingress egress	Mirrors ingress and egress packets.
<i>slot/port</i>	The slot and port number that will receive the mirrored traffic.

Defaults

parameter	default
ingress egress ingress egress	ingress

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove **mirror** from the policy action.
- Use this command to configure a mirror-to-port (MTP) action that is used for policy based mirroring.
- Only one MTP session is supported at any given time. As a result, all mirroring policies should specify the same MTP port.
- Policy based mirroring and the port based mirroring feature can run simultaneously on the same switch.

Examples

```
-> policy action a1 mirror 1/7 (default ingress)
-> policy action a1 ingress mirror 1/7
-> policy action a1 egress mirror 1/7
-> policy action a1 ingress egress mirror 1/7
-> policy action a1 no mirror
```

Release History

Release 7.1.1; 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  
  alaQoSActionMirrorSlot  
  alaQoSActionMirrorPort  
  alaQoSActionMirrorMode  
  alaQoSActionMirrorModeStatus
```

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.
<i>network_group</i>	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 10K, 6900

Usage Guidelines

Information for all policy network groups displays unless *network_group* is specified.

Examples

```
-> show policy network group
Group Name           : netg1
State                = new,
Entries              = 198.206.10.1
```

```
-> show policy network group
Group Name           : group1
Entries              = 203.185.129.0 mask 255.255.255.0,
                    203.185.131.192 mask 255.255.255.192,
                    203.185.132.0 mask 255.255.252.0,
                    204.226.0.0 mask 255.255.0.0
```

output definitions

Group Name	The name of the port group, configured through the policy network group command.
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Entries	The IP addresses associated with the network group.

Release History

Release 7.1.1; 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.
<i>service_name</i>	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 10K, 6900

Usage Guidelines

Information about all policy services is displayed unless *service_name* is specified.

Examples

```
-> show policy service
Service name           : s1
State                  = new,
Destination UDP port   = 1001-2004
```

output definitions

Service Name	The name of the port group, configured through the policy service command.
State	This field appears if the service was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
IPProto	The IP protocol associated with the service.
SrcPort	A source port associated with the service.
DstPort	A destination port associated with the service.

Release History

Release 7.1.1; 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.
<i>service_group</i>	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 10K, 6900

Usage Guidelines

Information for all policy service groups displays unless *service_group* is specified.

Examples

```
-> show policy service group
Group Name      : mgmt
State           = new,
Entries        = ftp,
                http,
                https,
                snmp,
                ssh,
                telnet
```

output definitions

Group Name	The name of the port group, configured through the policy service group command.
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Entries	The services associated with the group. Services are configured through the policy service command.

Release History

Release 7.1.1; 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.
<i>mac_group</i>	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 10K, 6900

Usage Guidelines

Information for all policy MAC groups displays unless *mac_group* is specified.

Examples

```
-> show policy mac group
Group Name      : mg1
State           = new,
Entries         = 00:02:9A:44:5E:10 mask 00:00:00:FF:FF:FF,
                00:11:01:00:00:01 mask 00:00:00:FF:FF:FF
                00:02:9A:44:5E:20
```

output definitions

Group Name	The name of the port group, configured through the policy mac group command.
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Entries	The MAC addresses associated with the group.

Release History

Release 7.1.1; command was introduced.

Related Commands

[policy mac group](#)

Configures policy MAC groups.

MIB Objects

alaQoSACGroupsTable

 alaQoSACGroupsName

 alaQoSACGroupsSource

alaQoSAppliedMACGroupsTable

 alaQoSAppliedMACGroupsName

 alaQoSAppliedMACGroupsSource

alaQoSACGroupTable

 alaQoSACGroupMacAddr

 alaQoSACGroupMacMask

alaQoSAppliedMACGroupTable

 alaQoSAppliedMACGroupMacAddr

 alaQoSAppliedMACGroupMacMask

show policy port group

Displays information about pending and applied policy port groups.

show [**applied**] **policy port group** [*group_name*]

Syntax Definitions

applied

Indicates that only policy port groups that have been applied should be displayed.

group_name

The name of the policy port group for which you want to display information; or a wildcard sequence of characters for displaying information about port groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Information for all policy port groups displays unless *group_name* is specified.

Examples

```
-> show policy port group
Group Name           : pg1
State                = new,
Entries              = 1/2,
                    1/3,
                    1/4,
                    3/11
```

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.).
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Entries	The slot/port combinations associated with the port group.

Release History

Release 7.1.1; command was introduced.

Related Commands

[policy port group](#)

Configures a port group and its associated slot and port numbers.

MIB Objects

```
alaQoSPortGroupsTable
  alaQoSPortGroupsName
  alaQoSPortGroupsSource
alaQoSAppliedPortGroupsTable
  alaQoSAppliedPortGroupsName
  alaQoSAppliedPortGroupsSource
alaPortGroupTable
  alaQoSPortGroupSlot
  alaQoSPortGroupPort
alaAppliedPortGroupTable
  alaQoSAppliedPortGroupSlot
  alaQoSAppliedPortGroupPort
```

show policy map group

Displays information about pending and applied policy map groups.

show [**applied**] **policy map group** [*group_name*]

Syntax Definitions

applied

Indicates that only map groups that have been applied should be displayed.

group_name

The name of the policy map group for which you want to display information; or a wildcard sequence of characters for displaying information about map groups with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Information for all policy map groups displays unless *group_name* is specified.

Examples

```
-> show policy map group
```

```
Group Name           : m1
State                = new,
Entries              = 0:0,
                    1:9,
                    2:18,
                    3:27,
                    4:36,
                    5:45,
                    6:54,
                    7:63
```

output definitions

Group Name	The name of the map group, configured through the policy map group command.
State	This field appears if the group was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Entries	The slot/port combinations associated with the port group.

Release History

Release 7.1.1; command was introduced.

Related Commands

[policy map group](#)

Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.

MIB Objects

```
alaQoSMapGroupsTable
  alaQoSMapGroupsName
  alaQoSMapGroupsSource
alaQoSAppliedMapGroupsTable
  alaQoSAppliedMapGroupsName
  alaQoSAppliedMapGroupsSource
alaQoSMapGroupTable
  alaQoSMapGroupKey
  alaQoSMapGroupKeyEnd
  alaQoSMapGroupValue
alaQoSAppliedMapGroupTable
  alaQoSAppliedMapGroupKey
  alaQoSAppliedMapGroupKeyEnd
  alaQoSAppliedMapGroupValue
```

show policy action

Displays information about pending and applied policy actions configured on the switch.

show [applied] policy action [*action_name*]

Syntax Definitions

applied

Indicates that only actions that have been applied should be displayed.

action_name

The name of the action for which you want to display information; or a wildcard sequence of characters for displaying information about actions with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Information for all policy actions displays unless *action_name* is specified.

Examples

```
-> show policy action
Action name                : a1
  Committed Information Rate = 10.0M,
  Committed Burst size      = 5.00M,
  Peak Information Rate      = 20.0M,
  Peak Burst size           = 5.00M

Action name                : a2
  State                     = new,
  Disposition               = deny

Action name                : a3
  State                     = new,
  Priority                   = 7,

-> show applied policy action
Action name                : a1
  Committed Information Rate = 10.0M,
  Committed Burst size      = 5.00M,
  Peak Information Rate      = 20.0M,
  Peak Burst size           = 5.00M
```

output definitions

Action Name	The name of the action, configured through the policy action command.
State	This field appears if the action was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Policy Action Parameters	Displays the configured policy action parameters.

Release History

Release 7.1.1; 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 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.
<i>condition_name</i>	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 10K, 6900

Usage Guidelines

Information for all policy conditions displays unless *condition_name* is specified.

Examples

```
-> show policy condition
Condition name           : c1
  Source VLAN           = 1001

Condition name           : c2
  State                 = new,
  Source IP              = 10.2.2.1,
  Destination UDP port  = 17

-> show applied policy condition
Condition name           : c1
  Source VLAN           = 1001
```

output definitions

Condition Name	The name of the condition, configured through the policy condition command.
State	This field appears if the condition was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Policy Condition Parameters	Displays the configured policy condition parameters.

Release History

Release 7.1.1; command was introduced.

Related Commands

[policy condition](#)

Creates a policy condition. The condition determines what parameters the switch uses to classify incoming flows.

MIB Objects

```
alaQoSConditionTable
  alaQoSConditionName
  alaQoSConditionSource
  alaQoSConditionSourceSlot
  alaQoSConditionSourcePort
  alaQoSConditionSourcePortGroup
  alaQoSConditionDestinationSlot
  alaQoSConditionDestinationPort
  alaQoSConditionDestinationPortGroup
  alaQoSConditionSourceInterfaceType
  alaQoSConditionDestinationInterfaceType
  alaQoSConditionSourceMacAddr
  alaQoSConditionSourceMacMask
  alaQoSConditionSourceMacGroup
  alaQoSConditionDestinationMacAddr
  alaQoSConditionDestinationMacMask
  alaQoSConditionDestinationMacGroup
  alaQoSConditionSourceVlan
  alaQoSConditionDestinationVlan
  alaQoSCondition8021p
  alaQoSConditionSourceIpAddr
  alaQoSConditionSourceIpMask
  alaQoSConditionSourceNetworkGroup
  alaQoSConditionDestinationIpAddr
  alaQoSConditionDestinationIpMask
  alaQoSConditionDestinationNetworkGroup
  alaQoSConditionMulticastIpAddr
  alaQoSConditionMulticastIpMask
  alaQoSConditionMulticastNetworkGroup
  alaQoSConditionTos
  alaQoSConditionDscp
  alaQoSConditionTcpFlags
  alaQoSConditionIpProtocol
  alaQoSConditionSourceIpPort
  alaQoSConditionDestinationIpPort
  alaQoSConditionService
  alaQoSConditionServiceGroup
```

show active policy rule

Displays information about pending and applied policy rules that are active (enabled) on the switch.

show active [**bridged** | **routed** | **multicast**] **policy rule** [*rule_name*]

Syntax Definitions

bridged	Displays active rules that apply to bridged traffic.
routed	Displays active rules that apply to routed traffic.
multicast	Displays active rules that apply to multicast traffic.
<i>rule_name</i>	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 10K, 6900

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.

Examples

```
-> show active policy rule
Rule name           : r1
Condition name      = c1,
Action name         = a1,
Packets             = 4166772,
Bytes               = 266665728
```

output definitions

Rule name	The name of the policy rule, configured through the policy rule command.
State	This field appears if the rule was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Condition name	The name of the condition configured for this rule.

output definitions (continued)

Action name	The name of the action configured for this rule.
Packets	The number of packets that match this rule.
Bytes	The number of bytes that match this rule.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy rule Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSRuleTable
  alaQoSRuleName
  alaQoSRuleEnabled
  alaQoSRuleSource
  alaQoSRulePrecedence
  alaQoSRuleActive
  alaQoSRuleReflexive
  alaQoSRuleLog
  alaQoSRuleTrapEvents
  alaQoSRuleSave
  alaQoSRuleCondition
  alaQoSRuleAction
```

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.
<i>rule_name</i>	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 10K, 6900

Usage Guidelines

- Information for all rules is displayed unless *rule_name* is specified.
- Information for all rule types is displayed unless a keyword (**bridged**, **routed**, **multicast**) is specified.
- Use the [show active policy rule](#) command to display only active rules that are currently being enforced on the switch.

Examples

```
-> show policy rule
Rule name           : r1
  Condition name    = c1,
  Action name       = a1

Rule name           : r2
  State             = new,
  Condition name    = c2,
  Action name       = a1

Rule name           : r3
  State             = new,
  Condition name    = c2,
  Action name       = a2
```

```
-> show applied policy rule
Rule name           : r1
  Condition name    = c1,
  Action name       = a1
```

output definitions

Rule name	The name of the policy rule, configured through the policy rule command.
State	This field appears if the rule was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
Condition name	The name of the condition configured for this rule.
Action name	The name of the action configured for this rule.

Release History

Release 7.1.1; command was introduced.

Related Commands

policy rule Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

```
alaQoSRuleTable
  alaQoSRuleName
  alaQoSRuleEnabled
  alaQoSRuleSource
  alaQoSRulePrecedence
  alaQoSRuleActive
  alaQoSRuleReflexive
  alaQoSRuleLog
  alaQoSRuleTrapEvents
  alaQoSRuleSave
  alaQoSRuleCondition
  alaQoSRuleAction
```

show policy validity period

Displays information about policy validity periods.

show policy validity period [*name*]

Syntax Definitions

name The name of the validity period.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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
Validity period name   = tuesday
  State                = new,
  Days                 = tuesday

Validity period name   = february
  Months               = february

-> show applied policy validity-period
Validity period name   = february
  Months               = february
```

output definitions

Validity period name	The name of the policy validity period, configured through the policy validity period command.
State	This field appears if the validity period was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
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.

output definitions

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 7.1.1; command was introduced.

Related Commands

policy validity period Configures a validity period that specifies days, times, and/or months during which an associated policy rule is in effect.

MIB Objects

```

alaQoSValidityPeriodTable
  alaQoSValidityPeriodName
  alaQoSValidityPeriodSource
  alaQoSValidityPeriodDays
  alaQoSValidityPeriodDaysStatus
  alaQoSValidityPeriodMonths
  alaQoSValidityPeriodMonthsStatus
  alaQoSValidityPeriodHour
  alaQoSValidityPeriodHourStatus
  alaQoSValidityPeriodEndHour
  alaQoSValidityPeriodInterval
  alaQoSValidityPeriodIntervalStatus
  alaQoSValidityPeriodEndInterval
alaQoSAppliedValidityPeriodTable
  alaQoSAppliedValidityPeriodName
  alaQoSAppliedValidityPeriodSource
  alaQoSAppliedValidityPeriodDays
  alaQoSAppliedValidityPeriodDaysStatus
  alaQoSAppliedValidityPeriodMonths
  alaQoSAppliedValidityPeriodMonthsStatus
  alaQoSAppliedValidityPeriodHour
  alaQoSAppliedValidityPeriodHourStatus
  alaQoSAppliedValidityPeriodEndHour
  alaQoSAppliedValidityPeriodInterval
  alaQoSAppliedValidityPeriodIntervalStatus
  alaQoSAppliedValidityPeriodEndInterval

```

show active policy list

Displays information about applied policy lists that are active (enabled) on the switch.

show active policy list [*list_name*]

Syntax Definitions

list_name

The name of the list for which you want to display information; or a wildcard sequence of characters for displaying information about lists with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

OmniSwitch 6900

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 7.2.1; 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 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 6900

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 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 7.2.1; 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

```

30 Policy Server Commands

This chapter describes CLI commands used for managing policies downloaded to the switch from an attached LDAP server. Policy rules can be created on an attached server through the PolicyView GUI application. Policy rules can also be created on the switch directly through CLI or SNMP commands. This chapter describes commands related to managing LDAP policies only. See [Chapter 28, “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 10K, 6900

Usage Guidelines

Policies are downloaded to the switch from the directory server with the highest preference setting; this server must be enabled and operational (able to bind).

Examples

```
-> policy server load
```

Release History

Release 7.1.1; command 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 10K, 6900

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 7.1.1; command 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-state** {**enable** | **disable**}] [**preference** *preference*]
[**user** *user_name* **password** *password*] [**searchbase** *search_string*] [**ssl** | **no ssl**]

no policy server *ip_address* [**port** *port_number*]

Syntax Definitions

<i>ip_address</i>	The IP address of the LDAP-enabled directory server.
<i>port_number</i>	The TCP/IP port number used by the switch to connect to the directory server.
enable	Enables the specified policy server to download rules to the switch. The policy servers are up by default.
disable	Prevents the specified policy server from downloading rules to the switch.
<i>preference</i>	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.
<i>user_name</i>	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: (e.g. “Directory Manager”).
<i>password</i>	The password associated with the user name. The password must match the password defined on the directory server.
<i>search_string</i>	The root of the directory required for searching the policy information. Typically, the <i>search_string</i> 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
<i>port_number</i>	389 (SSL disabled) 636 (SSL enabled)
<i>preference</i>	0
ssl no ssl	no ssl

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you change the port number, another entry is added to the policy server table; the 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 7.1.1; command 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 can be downloaded to the switch.

show policy server

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays basic information about policy servers. Use the **show policy server long** command to display more details about the servers.

Examples

```
-> show policy server
```

```
Server  IP Address  port  enabled  status  primary
-----+-----+-----+-----+-----+-----
   1    208.19.33.112  389    Yes     Up      X
   2    208.19.33.66   400    No      Down    -
```

output definitions

Server	The index number corresponding to the LDAP server.
IP Address	The IP address of the LDAP server.
port	The TCP/IP port number used by the switch to connect to the policy server.
enabled	Whether or not the policy server is enabled.
status	The state of the policy server, Unkn , Up or Down .
primary	Indicates whether the server is the primary server; this server can be used for the next download of policies; only one server is a primary server.

Release History

Release 7.1.1; command 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 10K, 6900

Usage Guidelines

This command displays detailed information about policy servers. Use the **show policy server** command to display basic information about policy servers.

Examples

```
-> show policy server long
LDAP server 0
  IP address       : 155.132.44.98,
  TCP port        : 16652,
  Enabled         : Yes,
  Operational status : Unkn,
  Preference      : 99,
  Authentication  : password,
  SSL             : Disabled,
  login DN       : cn=Directory Manager,
  searchbase     : ou:4.1, cn=policyRoot, o=company.fr
  Last load time  : 09/13/01 16:38:18
LDAP server 1
  IP address       : 155.132.48.27,,
  TCP port        : 21890,
  Enabled         : Yes,
  Operational status : Unkn,
  Preference      : 50,
  Authentication  : password,
  SSL             : Disabled,
  login DN       : cn=Directory Manager,
  searchbase     : o=company.fr
  Last load time  : 00/00/00 00:00:00
```

output definitions

IP address	The IP address of the policy server.
TCP port	The TCP/IP port number used by the switch to connect to the policy server.

output definitions (continued)

Enabled	Displays whether the policy server is enabled through 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 can 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 7.1.1; command 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 10K, 6900

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 7.1.1; command 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 from a directory server, that have been downloaded to the switch.

show policy server rules

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays information about policies created on directory servers only. [Chapter 28, “QoS Commands,”](#) for information about configuring and displaying policies directly on the switch.

Examples

```
-> show policy server rules
Num      name          prio      scope      status
-----+-----+-----+-----+-----
1         QoSRule1       0         Provisioned Active
2         QoSrule2       0         Provisioned Active
```

Fields are defined here:

output definitions

Num	An index number corresponding to the policy rule.
name	The name of the policy rule; only rules configured through PolicyView are displayed in this table.
prio	The priority or preference of the rule. Indicates the order in which rules can be checked to match to the incoming traffic. If two or more rules apply to the traffic, the rule with the highest preference is applied. Preference is determined when the rule is created.
scope	The type of rule. Provisioned is the only type valid for the current release.
status	The status of the rule: Active indicates that the rule has been pushed to is available in the QoS software on the switch and is available to be applied to the traffic; notInService means the rule can be pushed to the QoS software in the future but is not available yet (typically because of a variable validity period); notReady indicates that the rule can never be pushed to the QoS software because its validity period has expired or because it has been disabled through SNMP.

Release History

Release 7.1.1; command introduced.

Related Commands

[policy server load](#)

Downloads policies from a LDAP server. These policies are created through the PolicyView management application.

MIB Objects

```
policyRuleNamesTable  
  policyRuleNamesIndex  
  policyRuleNamesName  
  policyRuleOperStatus
```

show policy server events

Displays any events related to a directory server on which policies are stored.

show policy server events

Syntax Definitions

N/A

Defaults

The display is limited to 50 events.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The Policy Manager initialization event is always the first event logged.

Examples

```
-> show policy server events
Event Time                event description
-----+-----
09/13/01 16:38:15 Policy manager log init
09/13/01 16:38:17 LDAP server 155.132.44.98/16652 defined
09/13/01 16:38:17 LDAP server 155.132.44.98/21890 defined
09/13/01 16:38:18 PDP optimization: PVP day-of-week all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 PDP optimization: PVP Month all 1
09/13/01 16:38:18 IP address and mask make bad address change on desination IP
address 155.132.44.98:155.132.44.101
```

:

output definitions

Event Time	The date and time the policy event occurred.
event description	A description of the event.

Release History

Release 7.1.1; command 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
```

31 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 information may be stored locally in the switch user database.
- **Local user database.** User information may be configured for Authenticated Switch Access. For functional management access, users may be allowed to access specific command families or domains.

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 tacacs+-server aaa ldap-server show aaa server
Authenticated Switch Access	aaa authentication aaa authentication default aaa accounting session aaa accounting command show aaa authentication show aaa accounting
Port-based Network Access Control	aaa device-authentication mac show aaa device-authentication
Local User Database and Partitioned Management	user password user password-size min user password-expiration show user show aaa priv hexa

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-policy
------------------------	--

User Lockout Settings	user lockout-window user lockout-threshold user lockout-duration user lockout unlock show user show user lockout-setting
------------------------------	---

aaa radius-server

Configures or modifies a RADIUS server for Authenticated Switch Access.

```
aaa radius-server server [host {hostname | ip_address} [hostname2 | ip_address2]] [key secret]
[retransmit retries] [timeout seconds] [auth-port auth_port] [acct-port acct_port] [vrf-name name]
```

```
no aaa radius-server server
```

Syntax Definitions

<i>server</i>	The name of the RADIUS server.
<i>hostname</i>	The host name (DNS name) of the primary RADIUS server. The host name or IP address is required when creating a server.
<i>ip_address</i>	The IP address of the primary RADIUS server. An IP address or host name is required when creating a server.
<i>hostname2</i>	The host name (DNS name) of an optional backup RADIUS server.
<i>ip_address2</i>	The IP address of an optional backup RADIUS server.
<i>secret</i>	The shared secret known to the switch and the server, but which is not sent over the network. Can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case-sensitive. Required when creating a server.
<i>retries</i>	The number of retries the switch makes to authenticate a user before trying the backup server (<i>hostname2</i> or <i>ip_address2</i>).
<i>seconds</i>	The timeout for server replies to authentication requests.
<i>auth_port</i>	The UDP destination port for authentication requests.
<i>acct_port</i>	The UDP destination port for accounting requests.
<i>name</i>	The name of the VRF to be used to access the server.

Defaults

parameter	default
<i>retries</i>	3
<i>seconds</i>	2
<i>auth_port</i>	1812
<i>acct_port</i>	1813

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A host name (or IP address) and a secret are required when configuring a server.
- The server and the backup server must both be RADIUS servers.
- Use the **no** form of the command to remove a RADIUS server from the configuration. Only one server can be deleted at a time.
- RADIUS server can be configured on any VRF instance or the default VRF instance. However, all the RADIUS servers must reside on the same VRF instance.

Examples

```
-> aaa radius-server pubs2 host 10.10.2.1 key wwtoe timeout 5  
-> no aaa radius-server pubs2
```

```
-> aaa radius-server radsrv1 host rad1_ipaddr key rad1_secret vrf-name rad_vrf
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show aaa server	Displays information about AAA servers.
aaa authentication	Specifies the AAA servers to be used for Authenticated Switch Access.
aaa accounting session	Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

```
aaaServerTable  
  aaasProtocol  
  aaasHostName  
  aaasIpAddress  
  aaasHostName2  
  aaasIpAddress2  
  aaasRadKey  
  aaasRetries  
  aaasTimeout  
  aaasRadAuthPort  
  aaasRadAcctPort  
  aaasVrfName
```

aaa 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]
[timeout seconds] [port port] [vrf-name name]
```

```
no aaa tacacs+-server server
```

Syntax Definitions

<i>server</i>	The name of the TACACS+ server.
<i>hostname</i>	The host name (DNS name) of the primary TACACS+ server. The host name or IP address is required when creating a server.
<i>ip_address</i>	The IP address of the primary TACACS+ server. An IP address or host name is required when creating a server.
<i>hostname2</i>	The host name (DNS name) of an optional backup TACACS+ server.
<i>ip_address2</i>	The IP address of an optional backup TACACS+ server.
<i>secret</i>	The shared secret known to the switch and the server, but which is not sent over the network. Can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case-sensitive. required when creating a server.
<i>seconds</i>	The timeout for server replies to authentication requests.
<i>port</i>	The port number for the primary TACACS+ server.
<i>name</i>	The name of the VRF to be used to access the server.

Defaults

parameter	default
<i>seconds</i>	2
<i>port</i>	49

Platforms Supported

OmniSwitch 10K, 6900

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.
- The server and the backup server must both be TACACS+ servers.

- TACACS+ server can be configured on any VRF instance or the default VRF instance. However, all the TACACS+ servers must reside on the same VRF instance.

Examples

```
-> aaa tacacs+-server tpub host 10.10.2.2 key otna timeout 10
-> no aaa tacacs+-server tpub
-> aaa tacacs+-server tacsv1 host tacl_ipaddr key tacl_secret vrf-name tac_vrf
```

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **vrf-name** parameter added.

Related Commands

show aaa server	Displays information about AAA servers.
aaa authentication	Specifies the AAA servers to be used for Authenticated Switch Access.
aaa accounting session	Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

```
aaaServerTable
  aaasName
  aaasProtocol
  aaasHostName
  aaasIpAddress
  aaasHostName2
  aaasIpAddress2
  aaasTacacsKey
  aaasTimout
  aaasTacacsPort
  aaasVrfName
```

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] [base search_base] [retransmit retries] [timeout seconds] [ssl | no ssl]
[port port] [vrf-name name]
```

```
no aaa ldap-server server-name
```

Syntax Definitions

<i>server_name</i>	The name of the LDAP server.
<i>hostname</i>	The host name (DNS) of the primary LDAP server. The host name or IP address is required when creating a new server.
<i>ip_address</i>	The IP address of the primary LDAP server.
<i>hostname2</i>	The host name (DNS) of the backup LDAP server.
<i>ip_address2</i>	The IP address of a backup host for the LDAP server.
<i>dn_name</i>	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 <i>search-base</i> name and must be in a format supported by the server. Required when creating a new server.
<i>super_password</i>	The super-user password recognized by the LDAP-enabled directory servers. The password may be clear text or hexadecimal format. Required when creating a new server.
<i>search_base</i>	The search base recognized by the LDAP-enabled directory servers. For example, o=company or c=country . Must be different from the <i>dn_name</i> . Required when creating a new server.
<i>retries</i>	The number of retries the switch makes to the LDAP server to authenticate a user before trying the backup server.
<i>seconds</i>	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.
<i>port</i>	The port number for the primary LDAP server and any backup server. Must match the port number configured on the server.
<i>name</i>	The name of the VRF to be used to access the server.

Defaults

Defaults for optional parameters are as follows:

parameter	default
<i>port</i>	389 (SSL disabled) 636 (SSL enabled)
<i>retries</i>	3
<i>seconds</i>	2
ssl no ssl	no ssl

Platforms Supported

OmniSwitch 10K, 6900

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.
- LDAP server can be configured on any VRF instance or the default VRF instance. However, all the LDAP servers must reside on the same VRF instance.

Examples

```
-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager password tpub base c=us
retransmit 4
-> aaa ldap-server omnivista host 1.2.3.4 dn "cn=DirMgr, o=alcatel.com" password
somepass base "ou=People, o=alcatel.com" vrf-name ldap_vrf
-> no aaa ldap-server topanga5
```

Release History

Release 7.1.1; command was introduced.

Release 7.3.1; **vrf-name** parameter added.

Related Commands

show aaa server	Displays information about AAA servers.
aaa authentication	Specifies the AAA servers to be used for authenticated switch access.
aaa accounting session	Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

```
aaaServerTable
  aaasProtocol
  aaasHostName
  aaasIpAddress
  aaasHostName2
  aaasIpAddress2
  aaasLdapPort
  aaasLdapDn
  aaasLdapPasswd
  aaasLdapSearchBase
  aaasLdapServType
  aaasRetries
  aaasTimeout
  aaasLdapEnableSsl
  aaasVrfName
```

aaa authentication

Configures the interface for Authenticated Switch Access and specifies the server(s) to be used. This type of authentication gives users access to manage the switch.

aaa authentication {**console** | **telnet** | **ftp** | **http** | **snmp** | **ssh** | **default**} *server1* [*server2...*] [**local**]

no aaa authentication [**console** | **telnet** | **ftp** | **http** | **snmp** | **ssh** | **default**]

Syntax Definitions

console	Configures Authenticated Switch Access through the console port.
telnet	Configures Authenticated Switch Access for any port used for Telnet.
ftp	Configures Authenticated Switch Access for any port used for FTP.
http	Configures Authenticated Switch Access for any port used for Web-based management.
snmp	Configures Authenticated Switch Access for any port used for SNMP.
ssh	Configures Authenticated Switch Access for any port used for Secure Shell.
default	Configures Authenticated Switch Access for any port using any service (telnet , ftp , etc.). Note that SNMP access is enabled only if an LDAP or local server is specified with the command.
<i>server1</i>	The name of the authentication server used for Authenticated Switch Access. At least one server is required. The server may be a RADIUS, TACACS+, LDAP, or the local user database. RADIUS, TACACS+, and LDAP server names are set up through the aaa radius-server , aaa tacacs+-server , and aaa ldap-server commands.
<i>server2...</i>	The names of backup servers for Authenticated Switch Access. Up to 3 backups may be specified (including local). These backups are only used if <i>server1</i> 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 <i>server1</i> .

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 10K, 6900

Usage Guidelines

- The server type may be RADIUS, TACACS+, LDAP, or the local user database. Up to 4 servers may be configured for an interface type; at least one is required. Each server name should be separated by a space.
- The switch uses *only the first available server* in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS, TACACS+, and LDAP servers may each have an additional backup specified through the [aaa radius-server](#), [aaa tacacs+-server](#), and [aaa ldap-server](#) commands.
- If the local switch database will be used as the only authentication server, specify **local** for *server1*. If **local** is specified as a backup server, it should be entered last in the list of servers. The local user database is always available if the switch is up.
- Only LDAP or the local database may be used for authenticated SNMP management.
- If Secure Shell (**ssh**) is enabled, Telnet and FTP should be disabled.

Examples

```
-> aaa authentication telnet pubs1
-> no aaa authentication telnet
-> aaa authentication default pubs2 pubs3
```

Release History

Release 7.1.1; command was introduced.

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.
show aaa server	Displays information about servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAuthSTable
  aaatsInterface
  aaasName
  aaatsName1
  aaatsName2
  aaatsName3
  aaatsName4
```

aaa authentication default

Sets the authenticated switch access type to the default server setting.

aaa authentication {console | telnet | ftp | http | snmp | ssh} default

Syntax Definitions

console	Configures the default Authenticated Switch Access server setting for the console port.
telnet	Configures the default Authenticated Switch Access server setting for Telnet.
ftp	Configures the default Authenticated Switch Access server setting for FTP.
http	Configures the default Authenticated Switch Access server setting for Web-based management.
snmp	Configures the default Authenticated Switch Access server setting for any port used for SNMP.
ssh	Configures the default Authenticated Switch Access server setting for any port used for Secure Shell.

Defaults

By default, the default Authenticated Switch Access server setting does not include any servers.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **aaa authentication** command to set the default servers.

Examples

```
-> aaa authentication telnet default  
-> aaa authentication default default
```

Release History

Release 7.1.1; command was introduced.

Related Commands

aaa radius-server	Configures or modifies a RADIUS server for Authenticated Switch Access.
aaa tacacs+-server	Configures or modifies an LDAP server for Authenticated Switch Access.
user	Configures user information for the local database on the switch.
show aaa server	Displays information about servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAuthSTable  
  aaatsName1  
  aaatsName2  
  aaatsName3  
  aaatsName4
```

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

<i>server1</i>	The name of the RADIUS, TACACS+, or LDAP server used for accounting of authenticated switch sessions. At least one server is required. RADIUS, TACACS+, and LDAP server names are set up through the aaa radius-server , aaa tacacs+-server , and aaa ldap-server commands.
<i>server2...</i>	The names of backup servers. Up to 3 backups may be specified (including local); each server name should be separated by a space. These backups are only used if <i>server1</i> 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.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to disable accounting for Authenticated Switch Access.
- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The servers may be RADIUS, TACACS+, LDAP servers, and/or the local Switch Logging facility.
- If **local** is specified as *server1*, the switch will **only** use the local Switching Logging facility for accounting.
- If **local** is specified as a backup, it should be entered last in the list of servers. The Switch Logging facility is always available if the switch is up.
- The switch uses **only the first available server** in the list for accounting. For example, if *server1* is not available, the switch will use *server2*.
- RADIUS, TACACS+, and LDAP servers may each have an additional backup specified through the [aaa radius-server](#), [aaa tacacs+-server](#), and [aaa ldap-server](#) commands.

Examples

```
-> aaa accounting session ldap1 radius2 local
-> no aaa accounting session
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show aaa accounting](#)

Displays information about accounting servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAcctsaTable
  aaacsName1
  aaacsName2
  aaacsName3
  aaacsName4
```

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

<i>server1</i>	The name of the TACACS+ server used for command accounting. At least one server is required. TACACS+ server names are set up through the aaa tacacs+-server commands.
<i>server2...</i>	The names of TACACS+ backup servers. Up to 3 backups may be specified; each server name should be separated by a space. These backups are only used if <i>server1</i> 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.

Defaults

Accounting is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to disable command accounting.
- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The servers can be only TACACS+ servers.
- The switch uses *only the first available server* in the list for accounting. For example, if *server1* is not available, the switch will use *server2*.
- TACACS+ server may each have an additional backup specified through the [aaa tacacs+-server](#) command.

Examples

```
-> aaa accounting command tacacs1 tacacs2 tacacs3
-> no aaa accounting command
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show aaa accounting](#)

Displays information about accounting servers configured for Authenticated Switch Access.

MIB Objects

```
aaaAcctCmdTable  
  aaacmdSrvName1  
  aaacmdSrvName2  
  aaacmdSrvName3  
  aaacmdSrvName4
```

aaa device-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-suplicants).

aaa device-authentication mac *server1* [*server2*] [*server3*] [*server4*]

no device-authentication mac

Syntax Definitions

<i>server1</i>	The name of the RADIUS authentication server used for MAC authentication. (<i>Note that only RADIUS servers are supported for MAC authentication.</i>) At least one server is required. RADIUS server names are set up through the aaa radius-server command.
<i>server2...server4</i>	The names of backup servers used for MAC authentication. Up to 3 backups may be specified; include a space between each server name. These backups are only used if <i>server1</i> 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 6900

Usage Guidelines

- Up to 4 RADIUS servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- Use the **no** form of this command to disable MAC authentication for the switch.
- The switch uses **only the first available server** in the list to check for user information. For example, if *server1* is not available, the switch will poll *server2*. If user information is not found on the first available server, the authentication request will fail.
- RADIUS servers may each have an additional backup specified through the [aaa radius-server](#) command.
- MAC authentication verifies the source MAC address of a device via a remote RADIUS server. Used to classify devices for the Universal Network Profile (UNP) feature, this method sends RADIUS frames to the server with the MAC address embedded in the username and password attributes.
- Use the [unp port](#) command to enable or disable ports for UNP classification based on MAC authentication.
- Multiple devices can be authenticated on a given UNP port. Each device MAC address received on the port is authenticated and learned separately.

Examples

```
-> aaa device-authentication mac rad1 rad2  
-> no aaa device-authentication mac
```

Release History

Release 7.2.1; 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. |
| unp port | Enables or disables UNP port-based access control on a port. |
| show aaa device-authentication | Displays information about the global 802.1X configuration on the switch. |

MIB Objects

```
AaaAuthDatable  
  aaaDaName1  
  aaaDaName2  
  aaaDaName3  
  aaaDaName4
```

user

Configures or modifies user entries in the local user database. Use the **no** form of the command to remove the user from the local database.

user *username* [**password** *password*] [**expiration** {*day* | *date*}] [**read-only** | **read-write** [*families...* / *domains...*] **all** | **none**]] [**no snmp** | **no auth** | **sha** | **md5** | **sha+des** | **md5+des**] [**console-only** {**enable** | **disable**}]

no user *username*

Syntax Definitions

<i>username</i>	The name of the user. Used for logging into the switch. Required to create a new user entry or for modifying a user. Maximum 63 characters.
<i>password</i>	The user's password in clear text or hexadecimal (corresponding to encrypted form). Required to create a new user entry. Maximum 47 characters.
<i>day</i>	The number of days before this user's current password expires. The range is 1 to 150 days.
<i>date</i>	The date (in the format <i>mm/dd/yyyy hh:mm</i>) 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.
<i>families</i>	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.
<i>domains</i>	Determines the command domains available to the user on the switch. Each domain should be separated by a space.
all	Specifies that all command families and domains are available to the user.
none	Specifies that no command families or domains are available to the user.
no snmp	Denies the specified user SNMP access to the switch.
no auth	Specifies that the user has SNMP access without any required SNMP authentication and encryption protocol.
sha	Specifies that the SHA authentication algorithm should be used for authenticating SNMP PDU for the user.
md5	Specifies that the MD5 authentication algorithm should be used for authenticating SNMP PDU for the user.
sha+des	Specifies that the SHA authentication algorithm and DES encryption standard should be used for authenticating and encrypting SNMP PDU for the user.

md5+des	Specifies that the MD5 authentication algorithm and the DES encryption standard should be used for authenticating and encrypting SNMP PDU for the user.
console-only enable	Enables console only access for the user <i>admin</i> .
console-only disable	Disables console only access for the user <i>admin</i> .

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.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- At least one user with SHA/MD5 authentication and/or DES encryption must be configured on the switch for SNMPv3 communication with OmniVista.
- 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.
- 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.)
- New users or updated user settings are saved *automatically*.

Examples

```
-> user techpubs password writer_pass read-only config
-> no user techpubs
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[password](#)

Configures the current user's password.

[show user](#)

Displays information about users configured in the local database on the switch.

MIB Objects

aaaUserTable

aaauPassword

aaauReadRight

aaauWriteRight

aaauSnmpLevel

aaauSnmpAuthKey

aaauPasswordExpirationDate

password

Configures the current user's password.

password

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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.
- 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.
- 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*.

Examples

```
-> password
enter old password: *****
enter new password: *****
reenter new password: *****
->
```

Release History

Release 7.1.1; 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.

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
<i>size</i>	6

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A.

Examples

```
-> user password-size min 9
```

Release History

Release 7.1.1; 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.

[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

<i>day</i>	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
<i>day</i> / disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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.
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 10K, 6900

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 7.1.1; 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-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
<i>number</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>number</i>	4

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
<i>days</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show user password-policy](#) Displays the global password policy configuration for the switch.

MIB Objects

```
aaaAsaConfig
  aaaAsaPasswordMinAge
```

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
```

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
<i>minutes</i>	0

Platforms Supported

OmniSwitch 10K, 6900

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 **issu slot**, **reload slot**, or **configuration snapshot** command to save user settings over a reboot.

Examples

```
-> user lockout-duration 60
-> user lockout-duration 0
```

Release History

Release 7.1.1; 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 username {lockout | unlock}
```

Syntax Definitions

<i>username</i>	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 10K, 6900

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*.

Examples

```
-> user j_smith lockout
-> user j_smith unlock
```

Release History

Release 7.1.1; 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
```

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**, **aaa tacacs+-server**, or **aaa ldap-server** commands.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you do not include a server name in the syntax, information for all servers is displayed.

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,
  VRF                  = default
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
  VRF                  = default
Server name = Tpub1
  Server type           = TACACS+,
  IP Address 1         = 10.10.5.1,
  Port                 = 3,
  Timeout (in sec)    = 2,
  Encryption enabled  = no
  VRF                  = default
```

```

-> 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,
  VRF                  = default

```

output definitions

Server name	The name of the 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 (LDAP, TACACS+, or RADIUS).
Host name	The name of the primary LDAP, TACACS+, or RADIUS host.
IP address	The IP address of the server.
Retry number	The number of retries the switch makes to authenticate a user before trying the backup server.
Timeout	The timeout for server replies to authentication requests.
Port	The port number for the primary LDAP or TACACS+ server.
Encryption enabled	The status of the encryption.
Domain name	The super-user or administrative distinguished name in the format recognized by the LDAP-enabled directory servers.
Search base	The search base recognized by the LDAP-enabled directory servers.
Authentication port	The UDP destination port for authentication requests.
Accounting port	The UDP destination port for accounting requests.
VRF	Name of the VRF associated with the server.

Release History

Release 7.1.1; command was introduced.

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 tacacs+-server	Configures or modifies an TACACS+ server for Authenticated Switch Access.

MIB Objects

```

aaaServerTable
  aaasName
  aaasHostName
  aaasIpAddress

```

```
aaasHostName2  
aaasIpAddress2  
aaasRadKey  
aaasRetries  
aaasTimeout  
aaasRadAuthPort  
aaasRadAcctPort  
aaasProtocol  
aaasTacacsKey  
aaasTacacsPort  
aaasLdapPort  
aaasLdapDn  
aaasLdapPasswd  
aaasLdapSearchBase  
aaasLdapServType  
aaasLdapEnableSsl  
aaasVRFName
```

show aaa authentication

Displays information about the current authenticated switch session.

show aaa authentication

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[aaa authentication](#) Configures the interface for Authenticated Switch Access and specifies the server(s) to be used.

MIB Objects

aaaAuthSatable
aaatsName1
aaatsName2
aaatsName3
aaatsName4

show aaa device-authentication

Displays a list of RADIUS servers configured for MAC-based authentication.

show aaa device-authentication

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

This command displays MAC authentication servers configured through the [aaa device-authentication mac](#) command.

Examples

```
-> show aaa device-authentication
1st 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 7.2.1; command was introduced.

Related Commands

[aaa device-authentication mac](#) Enables/disables the switch for MAC-based authentication.

MIB Objects

AaaAuthMACTable

aaaDaName1

aaaDaName2

aaaDaName3

aaaDaName4

show aaa accounting

Displays information about accounting servers configured for Authenticated Switch Access. 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 10K, 6900

Usage Guidelines

Use the **show aaa accounting** command to display accounting servers configured for management session types (Telnet, FTP, console port, HTTP, or SNMP).

Examples

```
-> show aaa accounting
    1st accounting server      = RadiusServer
    2nd accounting server     = local
```

output definitions

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 7.1.1; command was introduced.

Related Commands

[aaa accounting session](#) Configures accounting servers for Authenticated Switch Access sessions.

MIB Objects

```
aaaAcctSatable
  aaacsName1
  aaacsName2
  aaacsName3
  aaacsName4
```

output definitions

User name	The user name for this account.
Password expiration	The date and time on which the password will expire. This field only displays if the password expiration is configured specifically for a user, or a default password expiration is configured globally on the switch through the user password-expiration command. (Note that the date/time are based on the switch's default system date/time or the system date/time configured through the system date and system time commands.)
Password allow to be modified date	The earliest date and time on which the user may change the password. Configured through the user password-min-age command.
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.
Read/Write for domains	The command domains available with the user's read-write access. See the table on the next page for a listing of valid domains.
Read Only for families	The command families available with the user's read-only access. See the table on the next page for a listing of valid families.
Read/Write for families	The command families available with the user's read-write access. See the table on the next page for a listing of valid families.
Snmp 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 ospf bgp vrrp ip-routing ipx ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-policy	qos policy slb
domain-security	session avlan aaa

Release History

Release 7.1.1; 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
  aaauSnmpLevel
  aaauSnmpAuthkey
```

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 10K, 6900

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-non-alpha 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 7.1.1; command was introduced.

Related Commands

show user password-policy 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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[user lockout unlock](#)

Manually locks or unlocks a user account on the switch.

[show user](#)

Displays information about all users or a particular user configured in the local user database on the switch.

MIB Objects

aaaAsaConfig

aaaAsaLockoutWindow

aaaAsaLockoutDuration

aaaAsaLockoutThreshold

show 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 10K, 6900

Usage Guidelines

- Valid values for the family parameter are listed in the Corresponding Families column of the following table:

Domain	Corresponding Families
domain-admin	file telnet dshell debug
domain-system	system aip snmp rmon webmgt config
domain-physical	chassis module interface pmm health
domain-network	ip rip ospf bgp vrrp ip-routing ipx ipmr ipms
domain-layer2	vlan bridge stp 802.1q linkagg ip-helper
domain-service	dns
domain-policy	qos policy slb
domain-security	session avlan aaa

- Note that some command families may not be supported depending on the hardware platform you are running.
- If you do not specify a command family, hexadecimal values for all commands sets will display.

Examples

```

-> show aaa priv hexa
file           = 0x00000001 0x00000000,
telnet         = 0x00000008 0x00000000,
dshell         = 0x00000020 0x00000000,
debug          = 0x00000040 0x00000000,
domain-admin   = 0x00000069 0x00000000,

system         = 0x00000080 0x00000000,
aip            = 0x00000100 0x00000000,
snmp           = 0x00000200 0x00000000,
rmon           = 0x00000400 0x00000000,
webmgt         = 0x00000800 0x00000000,
config         = 0x00001000 0x00000000,
domain-system  = 0x00001F80 0x00000000,

chassis        = 0x00002000 0x00000000,
module         = 0x00004000 0x00000000,
interface      = 0x00008000 0x00000000,
pmm            = 0x00010000 0x00000000,
health         = 0x00040000 0x00000000,
domain-physical = 0x0005E000 0x00000000,

ip             = 0x00080000 0x00000000,
rip            = 0x00100000 0x00000000,
ospf           = 0x00200000 0x00000000,
bgp            = 0x00400000 0x00000000,
vrrp           = 0x00800000 0x00000000,
ip-routing     = 0x01000000 0x00000000,
ipx            = 0x02000000 0x00000000,
ipmr           = 0x04000000 0x00000000,
ipms           = 0x08000000 0x00000000,
domain-network = 0x0FF80000 0x00000000,

vlan           = 0x10000000 0x00000000,
bridge         = 0x20000000 0x00000000,
stp            = 0x40000000 0x00000000,
802.1q         = 0x80000000 0x00000000,
linkagg        = 0x00000000 0x00000001,
ip-helper      = 0x00000000 0x00000002,
domain-layer2  = 0xF0000000 0x00000003,

dns            = 0x00000000 0x00000010,
domain-service = 0x00000000 0x00000010,

qos            = 0x00000000 0x00000020,
policy         = 0x00000000 0x00000040,
slb            = 0x00000000 0x00000080,
domain-policy  = 0x00000000 0x000000E0,

session        = 0x00000000 0x00000100,
avlan          = 0x00000000 0x00000400,
aaa            = 0x00000000 0x00000800,
domain-security = 0x00000000 0x00000D00

-> show aaa priv hexa rip
0x00100000 0x00000000

```

Release History

Release 7.1.1; command was introduced.

Related Commands

[user](#)

Configures or modifies user entries in the local user database.

32 UNP Commands

The Universal Network Profile (UNP) feature provides administrators with the ability to define and apply network access control to specific types of devices by grouping such devices according to specific matching profile criteria. This allows network administrators to create virtual machine network profiles (vNPs) and profiles for user devices from a unified framework of operation and administration.

UNP is not limited to creating profiles to classify only certain types of devices. However, the following classification methods implemented through UNP functionality and profile criteria provide the ability to tailor profiles for specific devices (physical or virtual):

- MAC-based authentication using a RADIUS-capable server.
- Switch-wide classification rules to classify on source MAC or IP address (no authentication required).
- VLAN tag classification to create VLAN port associations based on the VLAN ID contained in device packets.
- Default UNP classification for untagged traffic or traffic not classified through other methods.

Basically, UNP provides a method for dynamically assigning network devices to VLAN domains. A profile consists of configurable attributes. When a device sends traffic that matches such attributes, the device is then assigned to a VLAN service associated with the UNP. The UNP may also specify a QoS/ACL policy list that is subsequently applied to device traffic associated with the UNP VLAN service.

Dynamic assignment of devices using UNP is achieved through port-based functionality that provides the ability to authenticate and classify device traffic. Authentication verifies the device identity and provides a UNP name. In the event authentication is not available or is unsuccessful, classification rules associated with the UNPs are applied to the traffic to determine the UNP VLAN service assignment.

This chapter provides information about configuring UNP port parameters and profile attributes through the Command Line Interface (CLI).

MIB information for the UNP commands is as follows:

Filename: ALCATEL-IND1-DA-MIB
Module: alcatelIND1DaMIB

A summary of the available commands is listed here:

UNP Global Configuration Commands	unp dynamic-vlan-configuration unp dynamic-profile-configuration unp auth-server-down-unp unp auth-server-down-timeout
UNP Profile Commands	unp vlan-profile unp classification mac-address unp classification mac-range unp classification ip-address unp classification vlan-tag

UNP Port Commands	unp port unp default-vlan-profile unp mac-authentication unp mac-authentication pass-alternate unp classification unp port trust-tag
--------------------------	---

UNP show commands	show unp show unp global configuration show unp classification show unp port show unp user
--------------------------	---

unp vlan-profile

Configures a VLAN classification profile that is used to provide role-based access to the switch. This type of Universal Network Profile (UNP) determines the VLAN ID a device can join and if any QoS policy rules are applied to control access to network resources.

unp vlan-profile *unp_name* **vlan** *vlan_id* [**qos-policy-list** *list_name*]

no unp vlan-profile *unp_name*

Syntax Definitions

<i>unp_name</i>	The name of the UNP.
<i>vlan_id</i>	The VLAN ID number to associate with the specified UNP. Devices classified with the UNP are assigned to the associated VLAN.
<i>list_name</i>	The name of a policy list to associate with the specified UNP. The policy list contains QoS policy rules/ACLs that are applied to devices classified with the UNP.

Defaults

By default, no QoS policy list is assigned to the profile.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a UNP from the switch configuration.
- Specifying a QoS policy list name that is inactive or does not already exist in the switch configuration is allowed. However, the list will remain inactive for the UNP until the list is enabled or configured using the QoS policy list commands.
- If the UNP dynamic VLAN configuration capability is enabled, a VLAN specified with this command that does not exist in the switch configuration is automatically created when the UNP is created.

Note. Dynamic VLANs are not saved in the VLAN section of the **boot.cfg** file. However, the **unp** commands to enable dynamic VLAN configuration and create a UNP are saved in the UNP section of the **boot.cfg** file. As a result, the VLAN is created again on the next switch bootstrap.

Examples

```
-> unp vlan-profile unp1 vlan 100 qos-policy-list "list1"  
-> unp vlan-profile unp2 vlan 200 qos-policy-list "bad-list"  
-> no unp vlan-profile unp1
```

Release History

Release 7.2.1; command was introduced.

Release 7.3.1; OmniSwitch 10K support added, **name** parameter changed to **vlan-profile**.

Related Commands

unp port	Enables UNP on a port.
unp dynamic-vlan-configuration	Configures the status of dynamic VLAN configuration for profiles created with a VLAN ID that does not exist.
policy rule	Configures a QoS policy rule.
policy list	Configures a QoS policy list.
show unp	Displays the profile configuration for the switch.

MIB Objects

```
alaDaUserNetProfileTable
  alaDaUserNetProfileName
  alaDaUserNetProfileVlanID
  alaDaUserNetProfileRowStatus
  alaDaUserNetProfileQosPolicyListName
```

unp port

Configures the status of UNP functionality on a port or link aggregate.

```
unp {port {slot/port[-port2]} | linkagg agg_id}
```

```
no unp {port slot/port[-port2]} | linkagg agg_id}
```

Syntax Definitions

slot/port[-port2] The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

agg_id The link aggregate ID number.

Defaults

By default, UNP is disabled on all ports and link aggregates.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the UNP configuration from a port or link aggregate.
- Any configuration change to a UNP-enabled port will flush all MAC addresses learned on that port. This applies only to CLI commands used to configure UNP port parameters.
- Enabling UNP is *not* supported on the following port types:
 - > 802.1q-tagged ports.
 - > MVRP ports.
 - > Port Mirroring destination ports (MTP).
 - > Port Mapping network ports.
 - > STP and ERP ports.
 - > Ports on which a static MAC address is configured.
 - > Ports on which dynamic Source Learning is disabled.
 - > VLAN Stacking (Ethernet Services NNI or UNI) ports.
 - > Edge Virtual Bridging (EVB) ports.
- UNP and Learned Port Security (LPS) are supported on the same port with the following conditions:
 - > When LPS is enabled or disabled on a UNP port, MAC addresses learned on that port are flushed.
 - > When both LPS and UNP are enabled on the same port, UNP first authenticates and classifies any MAC addresses received, then LPS rules are applied. If a MAC address violates any of the LPS rules for the port, the address may get filtered or the port violated even if UNP initially determined

the address was valid. In other words, LPS rules take precedence over UNP to determine if a MAC address is bridged or filtered on the port.

- If UNP classifies a MAC address as learning but LPS learns the address as filtering, an untagged packet will show as filtering in the default VLAN for the port and a tagged packet MAC will show as filtering in the specific tagged VLAN.
 - When a MAC address is filtered by LPS, the **show unp user** command will display “LPS-Blocked” as the classification source for that MAC address.
 - The LPS **port-security chassis** command and some options of the **port-security learning-window** command are not supported on UNP ports. For more information about these exceptions and other conditions for using UNP and LPS on the same port, see [Chapter 35, “Learned Port Security Commands,”](#) in this guide and the UNP and LPS chapters in the *OmniSwitch AOS Release 7 Network Configuration Guide*.
- There is no limit to the number of switch ports that can have UNP enabled.

Examples

```
-> unp port 2/1
-> unp port 1/5-10
-> unp linkagg 10
-> unp linkagg 2-5
-> no unp port 2/1
-> no unp linkagg 10
```

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R02; **linkagg** parameter added.
Release 7.3.1; OmniSwitch 10K support added.

Related Commands

unp vlan-profile	Configures a VLAN-based UNP. This type of profile is applied to traffic ingressing on regular UNP bridge ports.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
  alaDaUNPPortIfIndex
```

unp default-vlan-profile

Configures the name of an existing VLAN classification profile to serve as the default UNP for the specified UNP port or link aggregate.

unp {port *slot/port1*[-*port2*] | linkagg *agg_id*} **default-vlan-profile** *unp_name*

no unp {port *slot/port1*[-*port2*] | linkagg *agg_id*} **default-vlan-profile**

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot and port number (3/1) of a UNP-enabled port. Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i>	The link aggregate ID number.
<i>unp_name</i>	The name of an existing VLAN classification profile.

Defaults

By default, there is no default profile configured for UNP ports or link aggregates.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to remove the default UNP from the port configuration.
- This command is allowed only on UNP-enabled ports.
- The VLAN classification profile specified with this command must already exist in the switch configuration.
- The default UNP is used to classify devices on the port when one of the following conditions occur:
 - > UNP authentication and classification are not enabled on the port.
 - > MAC authentication fails.
 - > Device traffic does not match UNP classification rules.
 - > The UNP trust VLAN tag option (see **unp port trust-tag**) is enabled for the port, but the VLAN ID specified in the tag field of the device traffic does not exist.
 - > Untagged device traffic is not classified.

Examples

```
-> unp port 1/1 default-vlan-profile "Sales"
-> no unp port 1/1 default-vlan-profile
-> unp port 1/1-4 default-vlan-profile "Sales"
ERROR: Port 1/2 is not a unp port
ERROR: Port 1/3 is not a unp port
-> unp port 1/1 default-vlan-profile "BAD-UNP"
```

```
ERROR: UNP doesn't exist
-> no unp port 1/1-4 default-vlan-profile
-> unp linkagg 5 default-vlan-profile "VM1-Server1"
-> no unp linkagg 5 default-vlan-profile
```

Release History

Release 7.3.1; command was introduced.

Related Commands

unp vlan-profile	Configures a VLAN-based UNP. This type of profile is applied to traffic ingressing on regular UNP bridge ports.
unp port trust-tag	Configures whether or not a device is classified into an existing VLAN that matches the VLAN ID tag of the packets received from the device.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
  alaDaUNPPortIfIndex
  alaDaUNPPortDefaultProfileName
```

unp mac-authentication

Configures the status of MAC authentication for the specified UNP port. Enable this functionality to invoke MAC-based authentication for devices connected to the UNP port.

```
unp {port slot/port1[-port2] | linkagg agg_id} mac-authentication {enable | disable}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i>	Link aggregate ID number.
enable	Enables MAC authentication.
disable	Disables MAC authentication.

Defaults

By default, MAC authentication is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is only allowed on UNP-enabled ports.
- MAC-based authentication is supported only through a RADIUS server.
- An option exists to classify a device into an alternate UNP in the event successful MAC authentication does not return a UNP name.
- If MAC authentication fails, any classification rules configured for the UNP port are applied.
- If both UNP MAC authentication and classification (see [unp classification](#)) are not enabled on the UNP port, all MAC addresses received on that port are blocked unless a default UNP is configured and/or trust VLAN tag is enabled for the port.

Examples

```
-> unp port 1/1 mac-authentication enable
-> unp port 1/1 mac-authentication disable
-> unp linkagg 2 mac-authentication enable
-> unp linkagg 2 mac-authentication disable
```

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R02; **linkagg** parameter added.
Release 7.3.1; OmniSwitch 10K support added.

Related Commands

unp mac-authentication pass-alternate	Assigns the device to another UNP when successful MAC authentication does not return a UNP name.
unp classification	Configures the classification status for the UNP port.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable  
  alaDaUNPPortIfIndex  
  alaDaUNPPortMacAuthFlag
```

unp mac-authentication pass-alternate

Configures the name of an existing VLAN-based UNP to use as an alternate profile. A device is assigned to the alternate profile when successful MAC authentication does not return a UNP name.

```
unp {port slot/port1[-port2] | linkagg agg_id} mac-authentication pass-alternate vlan-profile  
unp_name
```

```
no unp {port slot/port1[-port2] | linkagg agg_id} mac-authentication pass-alternate
```

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i>	Link aggregate ID number.
vlan-profile	A VLAN-based profile name.
<i>unp_name</i>	The name of an existing VLAN-based UNP.

Defaults

By default, no alternate UNP is configured.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the alternate profile from the UNP port configuration.
- The UNP name specified with this command must already exist in the switch configuration.

Examples

```
-> unp port 1/1 mac-authentication pass-alternate vlan-profile Finance  
-> no unp port 1/1-3 mac-authentication pass-alternate  
-> unp linkagg 5 mac-authentication pass-alternate vlan-profile AltUNP  
-> no linkagg 5 mac-authentication pass-alternate
```

Release History

Release 7.2.1; command was introduced.

Release 7.2.1.R02; **linkagg** parameter added.

Release 7.3.1; OmniSwitch 10k support added, **unp-name** parameter changed to **vlan-profile**.

Related Commands

unp vlan-profile

Configures a VLAN-based UNP. This type of profile is applied to traffic ingressing on regular UNP bridge ports.

unp mac-authentication

Configures the MAC authentication status for the UNP port.

show unp port

Displays the UNP port parameter configuration.

MIB Objects

alaDaUNPPortTable

 alaDaUNPPortIfIndex

 alaDaUNPPortPassAltProfileName

unp classification

Configures the classification status for the specified UNP port. When enabled and MAC authentication is disabled or fails, UNP classification rules (MAC address, MAC address range, IP network address, or VLAN tag) are applied to the traffic received on the UNP port.

```
unp {port slot/port1[-port2] | linkagg agg_id} classification {enable | disable}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i>	Link aggregate ID.
enable	Enables classification.
disable	Disables classification.

Defaults

By default, classification is disabled on the UNP port.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is allowed only on UNP-enabled ports.
- UNP classification rules are applied if MAC authentication is disabled on the port, is enabled on the port but the RADIUS server is not configured, or MAC authentication fails.
- If untagged device traffic does not match any of the classification rules, the device is assigned to the default UNP configured for the port.
- If tagged device traffic does not match any of the classification rules and the trust VLAN tag option (see [unp port trust-tag](#)) is enabled for the port, the device is classified based on the VLAN tag if a VLAN matching the tag exists in the switch configuration.
- If both UNP MAC authentication and classification (see [unp mac-authentication](#)) are not enabled on the UNP port, all MAC addresses received on that port are blocked unless a default VLAN is specified and/or trust VLAN tag is enabled for the port.
- When classification is enabled for the port, UNP classification rules are applied in the following order of precedence:
 - > MAC address + VLAN tag
 - > MAC address
 - > MAC address range + VLAN tag
 - > MAC address range
 - > IP address + VLAN tag
 - > IP address
 - > VLAN tag

Examples

```
-> unp port 1/1 classification enable
-> unp port 1/1 classification disable
-> unp port 1/1-4 classification enable
ERROR: Port 1/3 is not a unp-port
-> unp linkagg 5 classification enable
-> unp linkagg 5 classification disable
```

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R01; **linkagg** parameter added.
Release 7.3.1; OmniSwitch 10K support added.

Related Commands

show unp classification	Displays the UNP classification rule configuration for the switch.
show unp port	Displays the UNP configuration for the port.

MIB Objects

```
alaDaUNPPortTable
  alaDaUNPPortIfIndex
  alaDaUNPPortClassificationFlag
```

unp port trust-tag

Configures the option of whether or not to trust the VLAN ID of a tagged packet to determine how the packet is classified.

```
unp port {port slot/port1[-port2] | linkagg agg_id} trust-tag {enable | disable}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i>	Link aggregate ID.
enable	Trust the VLAN ID tag.
disable	Do not trust the VLAN ID tag.

Defaults

By default, the VLAN tag is not trusted.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When this option is enabled, the device is classified into a VLAN when one of the following conditions occur:
 - MAC authentication passes, but the RADIUS server returns a UNP that does not exist in the switch configuration.
 - MAC authentication passes, but the RADIUS server does not return a UNP and the alternate UNP option is disabled for the port.
 - Device traffic does not match any of the classification rules configured for the UNP port.
 - The UNP VLAN obtained from the matching classification rule does not exist in the switch configuration.
 - Auth-Server-Down UNP option is used, but the VLAN associated with that UNP does not exist in the switch configuration.
- When the trust tag option is triggered on a UNP bridge port and a VLAN exists in the switch configuration that matches the VLAN tag, a VLAN-port-association (VPA) is created between the UNP port and the matching VLAN even if the matching VLAN is *not* associated with a UNP.
- Enabling the trust VLAN ID tag option provides an implicit method of VLAN tag classification that will accept tagged traffic matching any of the existing UNPs without the need to create specific classification rules for those profiles.

Examples

```
-> unp port 1/1 trust-tag enable
-> unp port 1/1 trust-tag disable
-> unp port 1/1-4 trust-tag enable
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.1; OmniSwitch 10K support added.

Related Commands

show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPPortTable
  alaDaUNPPortIfIndex
  alaDaUNPPortTrustTagStatus
```

unp classification mac-address

Defines a MAC address classification rule for the specified Universal Network Profile (UNP). If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

unp classification mac-address *mac_address* [**vlan-tag** *vlan_id*] **vlan-profile** *unp_name*

no unp classification mac-address *mac_address*

Syntax Definitions

<i>mac_address</i>	MAC address (e.g., 00:00:39:59:f1:0c).
<i>vlan_id</i>	A VLAN ID.
<i>unp_name</i>	The name of a VLAN classification profile.

Defaults

By default, no classification rules are defined for a UNP.

parameter	default
<i>vlan_id</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the MAC address rule. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- When configuring a MAC address classification rule, specify an optional VLAN tag.
- When a VLAN classification profile is configured for this rule, the rule is applied only to traffic ingressing on UNP bridge ports.
- Adding a rule does not cause a MAC address flush. If necessary, use the **no mac-learning** command to clear and re-learn any addresses after the rule is added.
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source MAC address *and* the VLAN ID tag.
- Untagged packets are only classified using the specified MAC address; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification mac-address 00:11:22:33:44:55 vlan-profile CustA
-> unp classification mac-address 00:11:22:33:44:56 vlan-tag 100 vlan-profile CustB
```

Release History

Release 7.2.1; command was introduced.

Release 7.3.1; Omniswitch 10K support added, **unp-name** parameter changed to **vlan-profile**.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp vlan-profile	Configures a VLAN-based UNP. This type of profile is applied to traffic ingressing on regular UNP bridge ports.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainMacRuleTable
  alaDaUNPCustDomainMacRuleAddr
  alaDaUNPCustDomainMacRuleVlanTag
  alaDaUNPCustDomainMacRuleProfileName
  alaDaUNPCustDomainMacRuleRowStatus
```

unp classification mac-range

Defines a MAC address range classification rule for the specified Universal Network Profile (UNP). If the source MAC address of the device traffic matches any address within the range of MAC addresses, the specified UNP is applied to the device. An optional VLAN ID tag parameter is also available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

unp classification mac-range *low_mac_address high_mac_address* [**vlan-tag** *vlan_id*] **vlan-profile** *unp_name*

no unp classification mac-range *low_mac_address high_mac_address*

Syntax Definitions

<i>low_mac_address</i>	MAC address that defines the low end of the range (e.g., 00:00:39:59:f1:00).
<i>high_mac_address</i>	MAC address that defines the high end of the range (e.g., 00:00:39:59:f1:90).
<i>vlan_id</i>	A VLAN ID.
<i>unp_name</i>	The name of a VLAN classification profile.

Defaults

By default, no classification rules are defined for a UNP.

parameter	default
<i>vlan_id</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a MAC address range rule. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- When configuring a MAC address range classification rule, specify an optional VLAN before specifying the UNP for which the rule will classify traffic.
- When a VLAN classification profile is configured for this rule, the rule is applied only to traffic ingressing on UNP bridge ports.
- Adding a rule does not cause a MAC address flush. If necessary, use the **no mac-learning** command to clear and re-learn any addresses after the rule is added.
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing a source MAC address within the specified range *and* the VLAN ID tag.
- Untagged packets are only classified using the specified MAC address range; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification mac-range 00:11:22:33:44:66 00:11:22:33:44:77 vlan-profile
CustA
-> unp classification mac-range 00:11:22:33:44:01 00:11:22:33:44:20 vlan-tag 200
vlan-profile CustB
```

Release History

Release 7.2.1; command was introduced.

Release 7.3.1; Omniswitch 10K support added, **unp-name** parameter changed to **vlan-profile**.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp vlan-profile	Configures a VLAN-based UNP. This type of profile is applied to traffic ingressing on regular UNP bridge ports.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainMacRangeRuleTable
  alaDaUNPCustDomainMacRangeRuleLoAddr
  alaDaUNPCustDomainMacRangeRuleHiAddr
  alaDaUNPCustDomainMacRangeRuleVlanTag
  alaDaUNPCustDomainMacRangeRuleProfileName
  alaDaUNPCustDomainMacRangeRuleRowStatus
```

unp classification ip-address

Defines an IP network address classification rule for the specified Universal Network Profile (UNP). If the source IP address of the device traffic matches the IP address defined for the rule, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

unp classification ip-address *ip_address* **mask** *subnet_mask* [**vlan-tag** *vlan_id*] **vlan-profile** *unp_name*

no unp classification ip-address *ip_address* **mask** *subnet_mask*

Syntax Definitions

<i>ip_address</i>	IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).
<i>subnet_mask</i>	An IP address mask to identify the IP subnet for the interface (supports class-less masking).
<i>vlan_id</i>	A VLAN ID.
<i>unp_name</i>	The name of a VLAN classification profile.

Defaults

- By default, the subnet mask is set to the default subnet mask value for the IP address class.
- By default, no classification rules defined for a UNP.

parameter	default
<i>vlan_id</i>	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove an IP network address rule. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- When configuring an IP network address classification rule, specify an optional VLAN tag before specifying the UNP for which the rule will classify traffic.
- When a VLAN classification profile is configured for this rule, the rule is applied only to traffic ingressing on UNP bridge ports.
- Adding a rule does not cause a MAC address flush. If necessary, use the **no mac-learning** command to clear and re-learn any addresses after the rule is added.
- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source IP address *and* the VLAN ID tag.
- Untagged packets are only classified using the specified IP address; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```
-> unp classification ip-address 10.1.1.1 vlan-profile CustA
-> unp classification ip-address 50.1.1.1 vlan-tag 300 vlan-profile CustB
```

Release History

Release 7.2.1; command was introduced.

Release 7.3.1; Omniswitch 10K support added, **unp-name** parameter changed to **vlan-profile**.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp vlan-profile	Configures a VLAN-based UNP. This type of profile is applied to traffic ingressing on regular UNP bridge ports.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainIpNetRuleTable
  alaDaUNPCustDomainIpNetRuleAddr
  alaDaUNPCustDomainIpNetRuleMask
  alaDaUNPCustDomainIpNetRuleVlanTag
  alaDaUNPCustDomainIpNetRuleProfileName
  alaDaUNPCustDomainIpNetRuleRowStatus
```

unp classification vlan-tag

Defines a VLAN tag classification rule for the specified Universal Network Profile (UNP). If the VLAN ID tag of the device traffic matches the VLAN ID defined for the rule, the specified UNP is applied to the device.

unp classification vlan-tag *vlan_id* [**tag-position** {**inner** | **outer**}] {**vlan-profile** *unp_name*

no unp classification vlan-tag *vlan_id*

Syntax Definitions

<i>vlan_id</i>	A VLAN ID.
inner	Classify by matching the specified rule VLAN ID to the inner VLAN tag of a double-tagged packet.
outer	Classify by matching the specified rule VLAN ID to the outer VLAN tag of the double-tagged packet.
vlan-profile <i>unp_name</i>	The name of a VLAN classification profile.

Defaults

By default, no classification rules are defined for a UNP.

parameter	default
inner / outer	inner

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a VLAN tag rule. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- When configuring VLAN tag classification rule, specify an optional VLAN tag before specifying the UNP for which the rule will classify traffic.
- When a VLAN classification profile is configured for this rule, the rule is applied only to traffic ingressing on UNP bridge ports.
- Adding a rule does not cause a MAC address flush. If necessary, use the **no mac-learning** command to clear and re-learn any addresses after the rule is added.
- Untagged packets are not classified with this rule if a VLAN ID tag is specified with this command.

Examples

```
-> unp classification vlan-tag 400 vlan-profile CustA
-> unp classification vlan-tag 300 tag-position inner vlan-profile CustB
```

Release History

Release 7.2.1; command was introduced.

Release 7.3.1; Omniswitch 10K support added, **tag-position** and **unp-name** parameter changed to **vlan-profile**.

Related Commands

unp classification	Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp vlan-profile	Configures a VLAN-based UNP. This type of profile is applied to traffic ingressing on regular UNP bridge ports.
show unp classification	Displays the UNP classification rule configuration.

MIB Objects

```
alaDaUNPCustDomainVlanTagRuleTable
  alaDaUNPCustDomainVlanTagRuleVlan
  alaDaUNPCustDomainVlanTagRuleTagPosition
  alaDaUNPCustDomainVlanTagRuleVlanProfileName
  alaDaUNPCustDomainVlanTagRuleRowStatus
```

unp dynamic-vlan-configuration

Configures the UNP status for dynamic VLAN configuration. When this functionality is enabled and the UNP is created with a VLAN that does not exist, the switch will dynamically create the VLAN at the time the UNP is created.

unp dynamic-vlan-configuration {enable | disable}

Syntax Definitions

enable	Enables dynamic VLAN configuration for UNPs.
disable	Disables dynamic VLAN configuration for UNPs.

Defaults

By default, dynamic VLAN configuration is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Note. Dynamic VLANs are not saved in the VLAN section of the **boot.cfg** file. However, the **unp** commands to enable dynamic VLAN configuration and create a UNP are saved in the UNP section of the **boot.cfg** file. As a result, the VLAN is created again on the next switch bootup.

- When dynamic VLAN configuration is disabled, creating a UNP with a VLAN that does not exist in the switch configuration is not allowed.
- The VLAN status and other port (non-UNP port) assignments for a dynamic UNP VLAN are configurable using standard VLAN commands. In addition, the STP status is configurable and enabled by default when the dynamic VLAN is created.
- A dynamic VLAN cannot be deleted using standard VLAN commands (**no vlan *vlan_id***).
- UNP dynamic VLANs are identified as a separate type of VLAN. The **vlan show** commands will display this type with the default name of “UNP-DYN-VLAN” and the designated type as “UNP Dynamic Vlan”.

Examples

```
-> unp dynamic-vlan-configuration enable
-> unp dynamic-vlan-configuration disable
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.1; Omniswitch 10K support added.

Related Commands

- unp vlan-profile** Configures a UNP in the switch configuration.
- show unp global configuration** Displays the dynamic VLAN configuration status for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration  
  alaDaUNPDynamicVlanConfigFlag
```

unp dynamic-profile-configuration

Configures the UNP status for dynamic profile configuration. When this functionality is enabled, a UNP profile is dynamically created based on specific traffic conditions.

unp dynamic-profile-configuration {enable | disable}

Syntax Definitions

enable	Enables dynamic profile configuration for UNPs.
disable	Disables dynamic profile configuration for UNPs.

Defaults

By default, dynamic profile configuration is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When dynamic profile configuration is enabled, a UNP profile is dynamically created when the trust VLAN tag option is enabled on the UNP port or link aggregate and one of the following conditions occurs:
 - A tagged packet received on the UNP port contains a VLAN tag that matches an existing MVRP VLAN in the switch configuration that is not assigned to a profile.
 - There is no matching VLAN in the switch configuration.
- Dynamically created profiles are saved in the **boot.cfg** file for the switch.
- By default, dynamically created profiles are automatically named **dynamic_profile_vlan_id**, where the VLAN ID is the ID of the VLAN contained in the packet tag.
- After the dynamic profile is created, changing the profile name, associated VLAN ID, or the QoS policy list is allowed. To avoid any confusion, change the profile name if the VLAN ID associated with the profile has changed.
- If the dynamic profile configuration option is enabled along with the dynamic VLAN configuration option, if the dynamic creation of a profile refers to a VLAN that is a MVRP VLAN, then the MVRP VLAN is automatically converted to a dynamic UNP VLAN (UNP-DYN-VLAN).

Examples

```
-> unp dynamic-profile-configuration enable
-> unp dynamic-profile-configuration disable
```

Release History

Release 7.2.1.R02; command was introduced.
Release 7.3.1; OmniSwitch 10K support added.

Related Commands

- unp vlan-profile** Configures a UNP in the switch configuration.
- unp dynamic-vlan-configuration** Configures the status of dynamic VLAN configuration. When enabled, UNP will create a VLAN at the time a profile is created that specifies a VLAN ID that does not exist in the switch configuration.
- show unp global configuration** Displays the dynamic profile configuration status for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration  
alaDaUNPDynamicProfileConfigFlag
```

unp auth-server-down-unp

Configures a UNP to which a device is classified if MAC authentication fails because the RADIUS server is unreachable.

unp auth-server-down-unp *unp_name*

no auth-server-down unp

Syntax Definitions

unp_name The name of the UNP.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the authentication server down UNP.
- When a device is classified into the UNP created with this command, a configurable authentication down timer is started. When the timer runs out, the device is removed from the UNP and the authentication and classification process is performed again for that same device.
- If the authentication server down UNP is removed, the authentication server down timer is also removed.

Examples

```
-> unp auth-server-down-unp unp1  
-> no unp auth-server-down-unp
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.1; OmniSwitch 10K support added.

Related Commands

unp auth-server-down-timeout Configures the value for the authentication server down timer.

show unp global configuration Displays the profile designated as the authentication server down UNP for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration  
  alaDaUNPAuthServerDownUnp
```

unp auth-server-down-timeout

Configures the authentication server down timer value. This timer value is applied to devices that were learned in the authentication server down UNP.

unp auth-server-down-timeout *seconds*

Syntax Definitions

seconds The number of seconds the authentication server down timer is active. The valid range is 10 to 1000 seconds.

Defaults

By default, the timeout value is set to 60 seconds.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When this timer expires, devices learned in the authentication server down UNP are cleared from that UNP and authenticated and classified again.
- When the authentication server down UNP is removed, the authentication server down timer is also cleared.

Examples

```
-> unp auth-server-down-timeout 500  
-> unp auth-server-down-timeout 60
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.1: OmniSwitch 10K support added.

Related Commands

unp auth-server-down-unp Configures a UNP to which a device is classified if MAC authentication fails because the RADIUS server is unreachable.

show unp global configuration Displays the authentication server down timeout value for the switch.

MIB Objects

```
alaDaUNPGlobalConfiguration  
alaDaUNPAuthServerDownTimeout
```

show unp

Displays the VLAN-based Universal Network Profile (UNP) configuration for the switch.

show unp [*unp_name* | **sync** | **out-of-sync** | **local**]

Syntax Definitions

<i>unp_name</i>	The name of the UNP to display.
sync	Displays the UNP configurations that are the same on both MLAG peer switches.
out-of-sync	Displays the UNP configurations that are not the same on both MLAG peer switches.
local	Displays the UNP configurations that are local to the switch.

Defaults

By default, all VLAN-based profiles are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Enter a UNP name with this command to display information for a specific UNP.
- The UNP configuration must be the same on both MLAG peer switches. The “MC Conf Status” field contents indicates whether or not the UNP configuration is consistent on both peer switches.
- Use the **sync**, **out-of-sync**, or **local** parameters with this command to specify which profiles to display based on the MLAG consistency of the UNP configuration. The following table indicates under which conditions the VLAN-based UNP configuration is considered “in sync”, “out-of-sync”, or “local”.

Sync	Out of Sync	Local
Profile name is the same on both peer switches, and profiles are configured with the same parameters.	<ul style="list-style-type: none"> • Profile names are the same on both peer switches, but profile parameters are different. • Profile is configured on only one peer switch and is assigned to an MLAG aggregate as a default UNP or a Pass Alternate UNP. • Profile is configured on only one peer switch and is assigned to a device ingress-ing on an MLAG aggregate. 	<ul style="list-style-type: none"> • Profile is configured on only one peer switch and is not assigned to an MLAG aggregate as a default UNP or a Pass Alternate UNP. • Profile is configured on only one peer switch and is not assigned to a device ingress-ing on an MLAG aggregate.

Examples

```
-> show unp
```

```
Name                Vlan  Policy List Name  Status  MC Conf Status
-----+-----+-----+-----+-----
Sales                100   list1              Active  Sync
Finance              1000  list2              Inactive Out Of Sync
```

```
-> show unp sync
```

```
Name                Vlan  Policy List Name  Status  MC Conf Status
-----+-----+-----+-----+-----
Sales                100   list1              Active  Sync
```

```
-> show unp Finance
```

```
Name                Vlan  Policy List Name  Status  MC Conf Status
-----+-----+-----+-----+-----
Finance              1000  list2              Inactive Out Of Sync
```

output definitions

Name	The name of the profile. Configured through the unp vlan-profile command.
Vlan	The VLAN ID associated with the profile. Configured through the unp vlan-profile command.
Policy List Name	The name of the QoS policy list associated with the profile. Configured through the unp vlan-profile command.
Status	The status of the profile (Active or Inactive). An active profile indicates devices are assigned to the profile VLAN.
MC Conf Status	The MCLAG consistency check status of the UNP configuration (Sync , Out-Of-Sync , or Local).

Release History

Release 7.2.1; command was introduced.

Release 7.2.1.R02; **sync**, **out-of-sync**, and **local** parameters added; **Status** and **MC Conf Status** fields added.

Release 7.3.1; OmniSwitch 10K support added.

Related Commands

show unp classification	Displays the UNP classification rule configuration for the switch.
show unp global configuration	Displays the UNP global parameter values configured for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUserNetProfileTable  
  alaDaUserNetProfileName  
  alaDaUserNetProfileVlanID  
  alaDaUserNetProfileRowStatus  
  alaDaUserNetProfileQosPolicyListName  
  alaDaUserNetProfileMCLagConfigStatus
```

show unip global configuration

Displays the configuration for global Universal Network Profile (UNP) parameter settings.

show unip global configuration

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Configuring a UNP setup in a Multi-Chassis Link Aggregation (MCLAG) configuration is supported, but the UNP configuration must be the same on both MCLAG peer switches. The “MC Conf Status” field contents (Sync or Out Of Sync) indicates whether or not the UNP configuration is consistent on both peer switches.
- The following table indicates under which conditions the UNP global configuration is considered in sync or out-of-sync (the Local status does not apply to global UNP parameters).

	Sync	Out of Sync	Local
Dynamic VLAN Configuration	Enabled on both peer switches or disabled on both peer switches.	Enabled on one peer switch, but disabled on the other peer switch.	N/A
Dynamic Profile Configuration	Enabled on both peer switches or disabled on both peer switches.	Enabled on one peer switch, but disabled on the other peer switch.	N/A
Authentication Server Down UNP	<ul style="list-style-type: none"> The same authentication server down UNP name is configured on both peer switches. There is no authentication server down UNP configured on either one of the two peer switches. 	<ul style="list-style-type: none"> The authentication server down UNP name is different on each peer switch. The authentication server down UNP is configured on only one of the peer switches. 	N/A
Authentication Server Down Timeout	<ul style="list-style-type: none"> The timer value is the same on both peer switches. There is no timer value configured on either one of the two peer switches (the default value was not changed). 	<ul style="list-style-type: none"> The time value is different on each peer switch The timer value is configured on only one of the peer switches. 	N/A

Examples

```
-> show unp global configuration
Dynamic Vlan Configuration      : Enabled,
MC Conf Status                  : Sync,
Dynamic Profile Configuration   : Enabled,
MC Conf Status                  : Sync,
Auth Server Down UNP           : SrvDownUNP,
MC Conf Status                  : Sync,
Auth Server Down Timeout (Sec) : 60
MC Conf Status                  : Sync,
```

```
-> show unp global configuration
Dynamic Vlan Configuration      : Disabled,
MC Conf Status                  : Sync,
Dynamic Profile Configuration   : Disabled,
MC Conf Status                  : Sync,
Auth Server Down UNP           : -,
MC Conf Status                  : Out Of Sync,
Auth Server Down Timeout (Sec) : -,
MC Conf Status                  : Out Of Sync,
```

output definitions

Dynamic Vlan Configuration	The status (Enabled or Disabled) of dynamic VLAN configuration. Configured through the unp dynamic-vlan-configuration command.
MC Conf Status	The MCLAG consistency check status for the global UNP configuration of this parameter (Sync or Out Of Sync). The status is displayed for each global UNP parameter option.
Dynamic Profile Configuration	The status (Enabled or Disabled) of dynamic profile configuration. Configured through the unp dynamic-profile-configuration command.
Auth Server Down UNP	The name of a UNP that a device is assigned to in the event the RADIUS server is unreachable. This feature is not configured if a UNP name does not appear in this field. Configured through the unp auth-server-down-unp command.
Auth Server Down Timeout	The amount of time, in seconds, that devices remain in the VLAN associated with the authentication server down UNP. Configured through the unp auth-server-down-timeout command.

Release History

Release 7.2.1; command was introduced.

Release 7.2.1.R02; **Dynamic Profile Configuration** and **MC Conf Status** fields added.

Release 7.3.1; OmniSwitch 10K supported.

Related Commands

show unp	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```
alaDaUNPGlobalConfiguration
  alaDaUNPDynamicVlanConfigFlag
  alaDaUNPDynamicVlanMCLagConfigStatus
  alaDaUNPDynamicProfileConfigFlag
  alaDaUNPDynamicProfileConfigMCLagConfigStatus
  alaDaUNPAuthServerDownUnp
  alaDaUNPAuthServerDownUNPMCLagConfigStatus
  alaDaUNPAuthServerDownTimeout
  alaDaUNPAuthServerDownTimeoutMCLagConfigStatus
```

show unp classification

Displays the UNP classification rule configuration for the switch.

```
show unp classification {mac-rule | mac-range-rule | ip-rule | vlan-tag-rule} [sync | out-of-sync | local]
```

Syntax Definitions

mac-rule	Display the MAC address rule configuration.
mac-range-rule	Displays the MAC address range rule configuration.
ip-rule	Displays the IP network address rule configuration.
vlan-tag-rule	Displays the VLAN tag rule configuration.
sync	Displays the UNP configurations that are the same on both MCLAG peer switches.
out-of-sync	Displays the UNP configurations that are not the same on both MCLAG peer switches.
local	Displays the UNP configurations that are local to the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Specifying one of the classification rule type parameters is required with this command.
- The UNP configuration must be the same on both MCLAG peer switches. The “MC Conf Status” field contents (Sync, Out Of Sync, or Local) indicates whether or not the UNP configuration is consistent on both peer switches.
- Use the **sync**, **out-of-sync**, or **local** parameters with this command to specify which profiles to display based on the MCLAG consistency of the UNP configuration. The following table indicates under which conditions the UNP configuration is considered in sync, out-of-sync, or local.

Sync	Out of Sync	Local
The classification rule, rule attributes, and the UNP name for the rule are the same on both peer switches.	<ul style="list-style-type: none"> Classification rule and attributes are the same on both peer switches, but the UNP name for the rule is different. Classification rule is configured on only one peer switch, but a device ingressing on an MCLAG aggregate is classified with the rule. 	Classification rule is configured on only one peer switch but UNP has not classified any device ingressing on an MCLAG aggregate with this rule.

Examples

```
-> show unip classification mac-rule
```

Customer Domain	MAC Address	UNP Name	SPB Profile Name	Vlan Tag	MC Cfg Sync
1	00:00:5e:2a:95:11	SLA-10	VNP-10	0	Local
2	00:0f:b5:46:d7:56	SLA-20	-	20	Local

```
-> show unip classification mac-range-rule
```

Customer Domain	Low MAC Address	High MAC Address	UNP Name	SPB Profile Name	VLAN Name Tag	MC Cfg Sync
0	00:11:22:33:44:66	00:11:22:33:44:77	CustC	-	0	Local
1	00:11:22:33:44:88	00:11:22:33:44:99	CustB	VNP-B	10	Local

```
-> show unip classification ip-rule
```

Customer Domain	IP Address	IP Mask	UNP Name	SPB Profile Name	VLAN Tag	MC Cfg Sync
0	1.1.1.4	255.0.0.0	-	VNP-1	0	Local
1	1.1.1.5	255.0.0.0	CustA	-	0	Local
2	10.172.50.1	255.255.0.0	SLA-1	SLA-1525	50	Local

```
-> show unip classification vlan-tag-rule
```

Customer Domain	VLAN Tag	Vlan Name	Profile Name	SPB Profile Name	Tag Position	MC Conf Status
1	200	CustB		SLA-200	Inner	Local

output definitions

Customer Domain

Not supported in the current release. The customer domain ID assigned to the classification rule for the specified profiles. The rule is applied to traffic ingressing on UNP ports that are assigned to the same domain ID.

MAC Address

The MAC address value to match for this profile rule. Configured through the [unip classification mac-address](#) command.

output definitions

Low MAC Address	The lowest and highest MAC address values used to specify a range of addresses to match for this rule. Configured through the unp classification mac-range command.
High MAC Address	
IP Address IP Mask	The IP network address and mask values to match for this rule. Configured through the unp classification ip-address
UNP Name	The name of the UNP VLAN profile. Configured through the unp vlan-profile command.
SPB Profile Name	<i>Not supported in the current release.</i> The name of the UNP service profile.
VLAN Tag	The VLAN ID value to match for this profile rule. This rule is also supported in combination with each of the other classification rules. Configured through the unp classification vlan-tag or as a parameter with the other classification rule commands.
MC Conf Status	The MCLAG consistency check status for the UNP configuration (Sync , Out-Of-Sync , or Local).

Release History

Release 7.2.1; command was introduced.

Release 7.2.1.R02; **sync**, **out-of-sync**, and **local** parameters added, **MC Conf Status** field added.

Release 7.3.1; OmniSwitch 10K support added.

Related Commands

show unp	Displays the UNP configuration for the switch.
show unp port	Displays the UNP configuration for the port.
show unp user	Displays information about the devices learned on a UNP port.

MIB Objects

```

alaDaUNPCustDomainMacRuleTable
  alaDaUNPCustDomainMacRuleAddr
  alaDaUNPCustDomainMacRuleProfileName
  alaDaUNPCustDomainMacRuleVlanTag
  alaDaUNPCustDomainMacRuleMCLagConfigStatus

alaDaUNPCustDomainMacRangeRuleTable
  alaDaUNPCustDomainMacRangeRuleLoAddr
  alaDaUNPCustDomainMacRangeRuleHiAddr
  alaDaUNPCustDomainMacRangeRuleProfileName
  alaDaUNPCustDomainMacRangeRuleVlanTag
  alaDaUNPCustDomainMacRangeRuleMCLagConfigStatus

alaDaUNPCustDomainIpNetRuleTable
  alaDaUNPCustDomainIpNetRuleAddr
  alaDaUNPCustDomainIpNetRuleMask
  alaDaUNPCustDomainIpNetRuleProfileName
  alaDaUNPCustDomainIpNetRuleVlanTag
  alaDaUNPCustDomainIpNetRuleMCLagConfigStatus

```

```
alaDaUNPCustDomainVlanTagRuleTable  
  alaDaUNPCustDomainVlanTagRuleVlan  
  alaDaUNPCustDomainVlanTagRuleTagPosition  
  alaDaUNPCustDomainVlanTagRuleVlanProfileName  
  alaDaUNPCustDomainVlanTagRuleMCLagConfigStatus
```

show unp port

Displays the UNP configuration for the port. Includes only ports and link aggregates for which UNP is enabled.

show unp {port *slot/port1*[-*port2*] | **linkagg** *agg_id*} [**sync** | **out-of-sync** | **local**]

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i>	Link aggregate ID.
sync	Displays the UNP configurations that are the same on both MLAG peer switches.
out-of-sync	Displays the UNP configurations that are not the same on both MLAG peer switches.
local	Displays the UNP configurations that are local to the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Configuring a UNP setup in a Multi-Chassis Link Aggregation (MLAG) configuration is supported, but the UNP configuration must be the same on both MLAG peer switches. The “MC Conf Status” field contents (Sync, Out Of Sync, or Local) indicates whether or not the UNP configuration is consistent on both peer switches.
- The UNP configuration must be the same on both MLAG peer switches. The “MC Conf Status” field contents (Sync, Out Of Sync, or Local) indicates whether or not the UNP configuration is consistent on both peer switches.
- Use the **sync**, **out-of-sync**, or **local** parameters with this command to specify which profiles to display based on the MLAG consistency of the UNP configuration. The following table indicates under which conditions the UNP configuration is considered in sync, out-of-sync, or local.

Show Command	Sync	Out of Sync	Local
show unp port	MLAG aggregates: the UNP configuration is the same on both peer switches.	MLAG aggregates: the UNP configuration is not the same on both peer switches.	All ports; all link aggregates that are not MLAG.
show unp port <i>slot/port</i>	N/A - ports always Local.	N/A - ports always local.	All ports.

Show Command	Sync	Out of Sync	Local
show unp linkagg <i>agg_id</i>	MCLAG aggregates: the UNP configuration is the same on both peer switches.	<ul style="list-style-type: none"> MCLAG aggregates: the UNP configuration is not the same on both peer switches. MCLAG aggregates: UNP is enabled on only one of the peer switches. 	Link aggregates are not MCLAG.

Examples

```
-> show unp port
      UNP   Port MC Conf
Port  Domain Type  Mac-Auth Classification Default Pass-Alternate Trust-Tag Status
-----+-----+-----+-----+-----+-----+-----+-----
 1/11     0 Bridge Disabled Disabled          -      -           Disabled Local
 1/12     0 Bridge Disabled Disabled          -      -           Disabled Local
 1/20     0 Bridge Disabled Disabled          -      -           Disabled Local
 1/21     0 Bridge Disabled Disabled          -      -           Disabled Local

-> show unp port
      UNP   Port MC Conf
Port  Domain Type  Mac-Auth Classification Default Pass-Alternate Trust-Tag Status
-----+-----+-----+-----+-----+-----+-----+-----
0/10     1 Bridge Enabled Enabled          Def-unp SPB-pass   Disabled Sync
0/12     2 Bridge Enabled Enabled          VLAN10  VLAN-pass   Enabled  Sync
```

output definitions

Port	The port or link aggregate on which UNP is enabled. Configured through the unp port command.
UNP Domain	<i>Not supported in the current release.</i> The customer domain ID assigned to the UNP port. Traffic ingressing on the port is classified with UNP profile rules that are assigned to the same domain ID.
Port Type	The type of UNP port (Bridge).
Mac-Auth	The status of MAC authentication (Enabled or Disabled) for the UNP port or link aggregate. Configured through the unp mac-authentication command.
Classification	The status of classification (Enabled or Disabled) for the UNP port or link aggregate. Configured through the unp classification command.
Default	The name of the default UNP assigned to the port or link aggregate. Configured through the unp default-vlan-profile command.
Pass-Alternate	The name of the MAC authentication pass alternate UNP assigned to the port or link aggregate. Configured through the unp mac-authentication pass-alternate command.
Trust-Tag	The status of the trust VLAN tag option for the UNP port or link aggregate. Configured through the unp port trust-tag command.
MC Conf Status	The MCLAG consistency check status for the UNP port or link aggregate. The status for ports is always set to Local , but the status for link aggregates is set to Sync , Out Of Sync , or Local .

Release History

Release 7.2.1; command was introduced.

Release 7.2.1.R02; **linkagg**, **sync**, **out-of-sync**, and **local** parameters added; **MC Conf Status** field added.

Release 7.3.1; OmniSwitch 10K support added, **Port Type** field added.

Related Commands

show unp

Displays the UNP configuration for the switch.

show unp user

Displays information about the devices learned on a UNP port.

MIB Objects

alaDaUNPPortTable

alaDaUNPPortIfIndex

alaDaUNPPortDefaultProfileName

alaDaUNPPortPassAltProfileName

alaDaUNPPortMacAuthFlag

alaDaUNPPortClassificationFlag

alaDaUNPPortTrustTagStatus

alaDaUNPPortMCLagConfigStatus

show unp user

Displays information about the MAC addresses learned on a UNP port or link aggregate.

show unp user [*mac_address*] [*slot/port[-port2]*] | **linkagg** *agg_id*] [**count**]

Syntax Definitions

<i>mac_address</i>	The device MAC address.
<i>slot/port[-port2]</i>	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id</i>	Link aggregate ID.
count	Displays the number of UNP users.

Defaults

By default, information is displayed for all learned devices on all UNP ports and link aggregates.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **count** parameter is used on its own or in combination with a specified port or link aggregate.
- Enter a slot and port number to display devices learned on a specific port.
- Use the **linkagg** parameter and an aggregate ID number to display devices learned on a specific link aggregate.
- A zero is displayed instead of a slot number to designate a link aggregate. For example “0/10” specifies the device was learned on aggregate ID number 10.

Examples

```
-> show unp user
Total users: 3
```

Port	Username	Mac address	User IP	Vlan	UNP	Status	Learning Source
1/1	00:00:00:00:00:01	00:00:00:00:00:01	10.0.0.1	10	Sales	Active	Local
1/1	00:80:df:00:00:02	00:80:df:00:00:02	10.0.0.2	20	Finance	Active	Local
1/2	00:80:df:00:00:03	00:80:df:00:00:03	20.0.0.5	30	-	Block	Local
0/10	00:80:df:00:00:04	00:80:df:00:00:04	30.0.0.5	30	-	Block	Remote
0/11	00:80:df:00:00:05	00:80:df:00:00:05	40.0.0.5	30	-	Active	Local

output definitions

Port	The port or link aggregate on which the MAC address was learned.
User Name/MAC Address	The MAC address of the device.
User IP	The IP network address of the device.

output definitions

VLAN	The UNP VLAN ID in which the device was classified.
UNP	The name of the UNP to which the device was assigned.
Status	The status of the device (Active or Blocked)
Learning Source	Indicates in an MCLAG configuration if the device was classified on the local switch (Local) or learned on the peer switch (Remote).

```

-> show unp user 00:00:00:00:00:01
Port                : 01/20,
Mac-address         : 00:00:00:00:00:01,
IP                  : 14.15.16.17,
Vlan                 : 300,
UNP                 : UNP3,
Login Timestamp     : 04/01/1970 18:45:26,
Authentication Type : Mac authentication,
Authentication Status : Authenticated,
Classification Source : RADIUS - Server UNP
Learning source     : Local

-> show unp user 00:11:11:00:00:12
Port                : 01/20,
Mac-address         : 00:11:11:00:00:12,
IP                  : 14.15.16.17,
Vlan                 : 100,
UNP                 : UNP1,
Login Timestamp     : 04/01/1970 18:49:04,
Authentication Type : Mac authentication,
Authentication Status : Authenticated,
Classification Source : RADIUS - Default UNP
Learning source     : Local

-> show unp user 00:11:22:33:44:93
Port                : 01/20,
Mac-address         : 00:11:22:33:44:93,
IP                  : 14.15.16.17,
Vlan                 : 400,
UNP                 : UNP4,
Login Timestamp     : 04/01/1970 18:43:11,
Authentication Type : Mac authentication,
Authentication Status : Failed,
Classification Source : Auth Fail - MAC Range Rule UNP
Learning source     : Local

-> show unp user 00:11:22:33:44:99
Port                : 01/20,
Mac-address         : 00:11:22:33:44:99,
IP                  : 14.15.16.17,
Vlan                 : 500,
UNP                 : UNP5,
Login Timestamp     : 04/01/1971 18:50:01,
Authentication Type : - ,
Authentication Status : - ,
Classification Source : Tag - MAC Rule UNP
Learning source     : Local

```

```

-> show unp user 00:11:22:33:44:99
Port                : 01/20,
Mac-address         : 00:11:22:33:44:99,
IP                  : 14.15.16.17,
Vlan                 : 500,
UNP                  : UNP5,
Login Timestamp     : 04/01/1971 18:50:01,
Authentication Type : Mac Authentication,
Authentication Status : Failed,
Classification Source : Auth-Server-Down UNP
Learning source     : Local

-> show unp user 00:11:22:33:44:9A
Port                : 01/21,
Mac-address         : 00:11:22:33:44:9A,
IP                  : 14.15.16.19,
Vlan                 : 1,
UNP                  : - ,
Login Timestamp     : - ,
Authentication Type : Mac Authentication,
Authentication Status : Failed,
Classification Source : Auth-Server-Down UNP - Blocked
Learning source     : Local

-> show unp user 00:11:22:33:44:9A
Port                : 0/10,
Mac-address         : 00:11:22:33:44:9A,
IP                  : 14.15.16.19,
Vlan                 : 1,
UNP                  : - ,
Login Timestamp     : - ,
Authentication Type : Mac Authentication,
Authentication Status : Failed,
Classification Source : Auth-Server-Down UNP - Blocked
Learning source     : Remote

-> show unp user 1/1-5 count
Total users: 3

-> show unp user count
Total users: 3

-> show unp user linkagg 11 count
Total users: 2

```

output definitions

Port	The port or link aggregate on which the MAC address was learned.
MAC Address	The MAC address of the device.
IP	The IP network address of the device.
VLAN	The UNP VLAN ID in which the device was classified.
UNP	The name of the UNP to which the device was assigned.
Login Timestamp	The date and time the device was learned.
Authentication Type	The type of authentication used (only MAC authentication supported).

output definitions

Authentication Status	The status of the authentication process (blank “–” , Authenticated , Failed , or In Progress).
Classification Source	Indicates how the device was classified.
Learning Source	Indicates in an MCLAG configuration if the device was classified on the local switch (Local) or learned on the peer switch (Remote).

The following is a list of possible values for the “Classification Source” field:

- > Pass alternate UNP
- > Pass alternate UNP - Blocked
- > Default UNP
- > Default UNP - Blocked
- > Server UNP
- > Server UNP - Blocked
- > Auth Fail - Default UNP
- > Auth Fail - Default UNP - Blocked
- > Auth Fail - MAC Rule UNP
- > Auth Fail - MAC Rule UNP - Blocked
- > Auth Fail - MAC Range Rule UNP
- > Auth Fail - MAC Range Rule UNP - Blocked
- > Auth Fail - IP Rule UNP
- > Auth Fail - IP Rule UNP - Blocked
- > MAC Rule UNP
- > MAC Rule UNP - Blocked
- > MAC + Vlan Tag UNP
- > MAC + Vlan Tag UNP - Blocked
- > MAC Range rule UNP
- > MAC Range rule UNP - Blocked
- > MAC Range + Vlan Tag UNP
- > MAC Range + Vlan Tag UNP - Blocked
- > IP Rule UNP
- > IP Rule UNP - Blocked
- > IP + Vlan Tag UNP
- > IP + Vlan Tag UNP - Blocked
- > Vlan Tag Rule UNP
- > Vlan Tag Rule UNP - Blocked
- > Trust Tag
- > No UNP Match – Blocked
- > Auth-Server Down UNP
- > Auth-Server Down UNP – Blocked.
- > LPS - Blocked.

Release History

Release 7.2.1; command was introduced.

Release 7.2.1.R02; **linkagg** parameter added; **Learning Source** field added.

Release 7.3.1; OmniSwitch 10K support added.

Related Commands**show unnp**

Displays the UNP configuration for the switch.

show unnp portDisplays the UNP configuration for the port.

33 Edge Virtual Bridging Commands

The OmniSwitch implementation of Edge Virtual Bridging (EVB) is based on the the 802.1Qbg IEEE Standard. EVB is activated only on the backbone edge switches in a Data Center network. EVB is used to automate the discovery of Virtual Machines and connect them to the correct network domains, either the backbone bridge service network, or the VLAN bridged network.

The Edge Virtual Bridging commands allow you to configure and view Virtual Bridge settings required to be setup on an Edge OmniSwitch.

MIB information for the Edge Virtual Bridging commands is as follows:

Filename: IEEE8021-EVBB-MIB.mib
Module: IEEE8021-EVBB-MIB

Filename: ALCATEL-IND1-EVB-MIB.mib
Module: ALCATEL-IND1-EVB-MIB

A summary of available commands is listed here:

Management Commands	evb type evb evb-ldp manual evb ecp default-ack-timer evb ecp default-max-retry evb vdp default-resource-wait-delay evb vdp default-keep-alive-timeout
Monitoring Commands	show evb show evb config show evb sbp-config show evb cdcp-status show evb s-channel show evb ecp-status

evb type

Enables or disables the EVB VLAN bridging functionality on a switch port or link aggregate.

evb {port *slot/port* | linkagg *linkagg_id*} type vlan-bridging

no evb {port *slot/port* | linkagg *linkagg_id*}

Syntax Definitions

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

agg_id The link aggregate ID number.

Defaults

By default, EVB is not enabled on switch ports.

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- Use the **no** form of this command to disable the EVB configuration on the specified port.
- This command designates the specified port or link aggregate as a EVB Station-facing Bridge Port (SBP) that will connect to an EVB server.

Examples

```
-> evb port 1/1 type vlan-bridging  
-> evb linkagg 2 type vlan-bridging
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show evb config](#) Displays the current EVB configuration on the switch.

MIB Objects

```
evbPortModeTable  
    evbPortId  
    evbPortMode
```

evb evb-lldp manual

Enables or disables manual operating configuration for OmniSwitch after obtaining the EVB TLV setting.

evb evb-lldp manual {enable | disable}

Syntax Definitions

enable	Enables local EVB TLV manual setting.
disable	Disables local EVB TLV manual setting.

Defaults

By default, the EVB LLDP manual setting is disabled.

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- When EVB LLDP manual is enabled, the operating configuration of the OmniSwitch is determined only by the local EVB TLV settings.
- When EVB LLDP manual is disabled, the operating configuration is automatically determined by comparing the local and remote EVB TLV settings.

Examples

```
-> evb evb-lldp manual enable
-> evb evb-lldp manual disable
```

Release History

Release 7.3.1; command introduced.

Related Commands

show evb config	Displays the current EVB configuration on the chassis.
show evb sbp-config	Displays the Virtual Station Interface (VSI) to Station-facing Bridge Port (SPB) mapping information.

MIB Objects

```
ieee8021BridgeEvbConfig
  ieee8021BridgeEvbSysEvbLldpManual
```

evb ecp default-ack-timer

Configures the default amount of time to wait to receive an acknowledgment (ACK) Edge Control Protocol (ECP) data packet.

evb ecp default-ack-timer *ack_timer*

Syntax Definitions

ack_timer The default wait timer value to receive an acknowledgment (ACK) Edge Control Protocol (ECP) data packet.

Defaults

By default, the default ACK timer value is set to 14 (approximately 163.84 milli seconds).

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

- The ECP operates between the EVB server and EVB OmniSwitch and provides reliable delivery of VSI Discovery and Configuration Protocol (VDP) PDUs.
- Use the following formula to get the real timer value from the ACK timer:

Timer (in milli seconds) = $10 \times 2^{\text{ack_timer}}$

Examples

```
-> evb ecp default-ack-timer 20
-> evb ecp default-ack-timer 14
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show evb config](#) Displays the current EVB configuration on the chassis.

MIB Objects

```
ieee8021BridgeEvbConfig
  ieee8021BridgeEvbECPAckTimer
```

evb ecp default-max-retry

Configures the maximum number of times the Edge Control Protocol (ECP) must be retransmitted if no acknowledgment (ACK) packet is received.

evb ecp default-max-retry *max-try*

Syntax Definitions

max-try The maximum number of times that the ECP retries a transmission if no ACK (acknowledgment packet) is received. The valid range is 0 to 7.

Defaults

By default, the maximum number of retries value is set to 3.

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

The retransmission of packets occurs only after the default ACK timer value has expired.

Once the maximum number of retries value is reached without success (no ACK packet received), then the transmit buffer is cleared.

Examples

```
-> evb ecp default-max-retry 5
-> evb ecp default-max-retry 3
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show evb config](#) Displays the current EVB configuration on the chassis.

MIB Objects

```
ieee8021BridgeEvbConfig
  ieee8021BridgeEvbECPMaxRetries
```

evb vdp default-resource-wait-delay

Configures the value for wait period to initialize the timer on the edge OmniSwitch when a VSI Discovery and Configuration Protocol (VDP) resource is waiting for a response.

evb vdp default-resource-wait-delay *delay*

Syntax Definitions

delay The amount of time to wait for a response.

Defaults

By default, the *delay* parameter value is 20 (approximately 10.48576 seconds).

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

Use the following formula to get the default-resource-wait-delay value:

Timer (in micro second) = 10 x 2 ^ *delay*

Examples

```
-> evb vdp default-resource-wait-delay 25  
-> evb vdp default-resource-wait-delay 20
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show evb config](#) Displays the current EVB configuration on the chassis.

MIB Objects

```
ieee8021BridgeEvbConfig  
    ieee8021BridgeEvbSysVdpDfltRsrcWaitDelay
```

evb vdp default-keep-alive-timeout

Configures the value to initialize the timer by the station VDP to determine when to transmit keep-alive messages.

```
evb vdp default-keep-alive-timeout ka_timeout
```

Syntax Definitions

ka_timeout The keep-alive value for the timer.

Defaults

By default, the default keep-alive timeout value is set to 20 (approximately 0.48576 seconds).

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

Use the following formula to get the real timer value from the default-keep-alive timeout:

Timer (in micro second) = $10 \times 2^{\text{ka_timeout}}$

Examples

```
-> evb vdp default-keep-alive-timeout 25
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show evb config](#) Displays the current EVB configuration on the chassis.

MIB Objects

```
ieee8021BridgeEvbConfig  
  ieee8021BridgeEvbSysVdpDfltReinitKeepAlive
```

show evb

Displays the EVB port and the port bridging type.

show evb [**port** *slot/port* | **linkagg** *linkagg_id*]

Syntax Definitions

slot/port Slot and port number of the EVB port.

linkagg_id Link aggregate ID of the EVB port.

Defaults

By default, the EVB port type is displayed for all ports and link aggregates.

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

Use the **port** or **linkagg** parameters with this command to display information for a specific port or link aggregate.

Examples

```
-> show evb port linkagg
Port      Bridging Type
-----+-----
0/1       VLAN
0/2       VLAN
```

```
-> show evb port
Port      Bridging Type
-----+-----
1/1       VLAN
1/2       VLAN
```

```
-> show evb port 1/2
Port      Bridging Type
-----+-----
1/2       VLAN
```

output definitions

Port	The slot/port number or link aggregate ID of the EVB port.
Bridging Type	Specifies the port type is (VLAN). Currently no other port types are supported.

Related Commands

evb type

Configures the EVB port type.

MIB Objects

evbPortModeTable

evbPortId

evbPortMode

show evb config

Displays the current EVB configuration on the switch.

show evb config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

NA

Examples

```
-> show evb config
```

```
Auto Port Mode:                Enabled
Auto Default Port Type:        Vlan-Bridging
No. of external ports:         102
EVB-LLDP TX:                   -
EVB-LLDP manual:               Disabled
EVB-LLDP GroupID-capable:      -
ECP default-ack-timer (msec):  14 (163.84)
ECP default-max-retry:         3
VDP resource-wait-delay (sec): 20 (10.48)
VDP keep-alive-timeout (sec):  20 (10.48)
```

output definitions

Auto Port Mode	The EVB auto mode status (Enabled or Disabled). <i>Not supported in the current release; the EVB port type is manually configured.</i>
Auto Default Port Type	The default port type setting in auto mode - Vlan-Bridging or Service-Access . <i>Not supported in the current release..</i>
No. of external ports	The number of external ports on the EVB.
EVB-LLDP TX	The EVB-LLDP transmission status (Enabled or Disabled). <i>Not supported in the current release.</i>
EVB-LLDP manual	The EVB-LLDP manual setting (Enabled or Disabled).
EVB-LLDP GroupID	The EVB-LLDP groupID capability status (Enabled or Disabled). <i>Not supported in the current release.</i>
ECP ack-timer (msec)	The EVB acknowledgement timer value in milli seconds.

output definitions (continued)

ECP max-retry	The value for the maximum number of times that the ECP is retransmitted if no acknowledgment (ACK) packet is received.
VDP resource-wait-delay (sec)	The VDP resource wait delay value in seconds.
VDP keep-alive-timeout (sec)	The VDP keep-alive timeout value in seconds.

Release History

Release 7.3.1; command introduced.

Related Commands

evb ecp default-ack-timer	Configures the default wait timer value to receive an acknowledgment (ACK) data packet.
evb ecp default-max-retry	Configures the maximum number of times that the ECP must be retransmitted if no acknowledgment (ACK) packet is received.
evb vdp default-resource-wait-delay	Configures the delay value to initialize the timer for VDP on the edge OmniSwitch when a resource is waiting for a response.
evb vdp default-keep-alive-timeout	Configures the value to initialize the timer by the station VDP to determine when to transmit keep-alive messages.

MIB Objects

```

ieee8021BridgeEvbConfig
  ieee8021BridgeEvbSysNumExternalPorts
  ieee8021BridgeEvbSysEvbLldpTxEnable
  ieee8021BridgeEvbSysEvbLldpManual
  ieee8021BridgeEvbSysEvbLldpGidEnable
  ieee8021BridgeEvbECPACKTimer
  ieee8021BridgeEvbECPMaxRetires
  ieee8021BridgeEvbSysVdpDfltRsrcWaitDelay
  ieee8021BridgeEvbSysVdpDfltReinitKeepAlive

```

show evb sbp-config

Displays the Virtual Station Interface (VSI) to Station-facing Bridge Port (SBP) mapping information.

show evb sbp-config [*slot/port* | **linkagg** *linkagg_id*]

Syntax Definitions

slot/port Specifies the switch slot and port number of the EVB port.

linkagg_id Specifies the link aggregate ID of the group of the EVB port.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

The *slot/port* and *linkagg_id* parameter values specify the port number or link aggregate ID number to display the EVB CDCP status. If no port number is specified, then the mapping for all ports is displayed.

Examples

```
-> show evb sbp-config
```

port	sbp	manual mode	resource wait delay	reinit keep alive	tout keep alive
1/1	10	enabled	10.48	10.48	11.6
1/1	20	enabled	10.48	10.48	11.6
1/2	33	enabled	10.48	10.48	11.6
1/3	40	enabled	10.48	10.48	11.6

```
-> show evb sbp-config port linkagg 1
```

port	SBP	manual mode	resource wait delay (usec)	reinit keep alive (usec)	tout keep alive (usec)
0/1	61472	disabled	10485760	10485760	17448960
0/1	61473	disabled	10485760	10485760	17448960

output definitions

port	Specifies the slot and port number of the EVB port.
sbp	Specifies the SBP ID.
manual mode	Specifies whether manual mode is enabled or disabled .
resource wait delay	Specifies the configured resource wait delay value in seconds.
reinit keep alive	Specifies the configured reinit keep alive value in seconds.
tout keep alive	Specifies the configured keep alive timeout value in seconds.

Release History

Release 7.3.1; command introduced.

Related Commands

- [evb evb-lldp manual](#) Enables or disables manual operating configuration for OmniSwitch after obtaining the EVB TLV setting.
- [show evb config](#) Displays the current EVB configuration on the chassis.

MIB Objects

```
ieee8021BridgeEvbSbpTable  
  ieee8021BridgeEvbSbpComponentID  
  ieee8021BridgeEvbSbpPortNumber  
  ieee8021BridgeEvbSbpLldpManual  
  ieee8021BridgeEvbSbpVdpOperRsrcWaitDelay  
  ieee8021BridgeEvbSbpVdpOperReinitKeepAlive  
  ieee8021BridgeEvbSbpVdpOperToutKeepAlive
```

show evb cdcp-status

Displays the S-channel discovery and configuration protocol (CDCP) status of Uplink Access Ports (UAP).

show evb cdcp-status [*slot/port*]

Syntax Definitions

slot/port Specifies the switch slot and port number of the Uplink Access Ports.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

The *slot/port* parameter specifies the port number to display the EVB CDCP status. If no port number is specified, then the EVB CDCP status is displayed for all the related ports.

Examples

```
-> show evb cdcp-status
```

Admin	CDCP State		No. of S-channel		S-VLAN allocated		
Port	state	local	remote	Max No.	operational	lowest	highest
1/1	enable	running	enabled	55	20	1001	1020
1/2	enable	down	disabled	55	10	1001	1010

output definitions

Admin Port	Slot and port number of UAP.
Admin port state	Administrative status of CDCP of UAP - enable or disable .
CDCP State - local	Local running state of CDCP - running or down .
CDCP State - remote	Remote state for S-channel - enabled or disabled .
No. of S-channel - Max No.	Number of S-channels supported by the bridge.
No. of S-channel - operational	Number of S-channels that can be used.
S-VLAN allocated - lowest	The lowest S-VLAN available for assignment by CDCP.
S-VLAN allocated - highest	The highest S-VLAN available for assignment by CDCP.

Release History

Release 7.3.1; command introduced.

Related Commands

- show evb config** Displays the current EVB configuration on the chassis.
- show evb** Displays the EVB port and its port bridging type.

MIB Objects

```
ieee8021BridgeEvbUAPConfigTable  
  ieee8021BridgePhyPort  
  ieee8021BridgeEvbUAPSchCdcAdminEnable  
  ieee8021BridgeEvbUAPSchOperState  
  ieee8021BridgeEvbSchCdcRemoteEnable  
  ieee8021BridgeEvbUAPSchAdminCDCPChanCap  
  ieee8021BridgeEvbUAPSchOperCDCPChanCap  
  ieee8021BridgeEvbUAPSchAdminCDCPSVIDPoolLow  
  ieee8021BridgeEvbUAPSchAdminCDCPSVIDPoolHigh
```

show evb s-channel

Displays the S-Channel information.

show evb s-channel [*slot/port*]

Syntax Definitions

slot/port Specifies the switch slot and port number of the chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

The *slot/port* parameter specifies the port number to display the S-channel configuration. If no port number is specified, then the S-channel configuration is displayed for all the related ports.

Examples

```
> show evb s-channel
```

```
Port  S-Ch Id   S-VLAN   SBP
-----+-----+-----+-----
1/1   1         1        20
1/1   2        1002     21
1/2   1         1        200
```

output definitions

Port	Specifies the slot and port number.
S-Ch ID	Specifies the S-Channel ID.
S-VLAN	Specifies the S-VLAN ID.
SBP	Specifies the Station-facing Bridge Port (SBP) number.

Release History

Release 7.3.1; command introduced.

Related Commands

`show evb cdcv-status`

Displays the S-channel Discovery and Configuration Protocol (CDCP) status of Uplink Access Ports (UAP).

MIB Objects

```
ieee8021BridgeEvbCAPConfigTable  
  Ieee8021BridgePhyPort  
  ieee8021BridgeEvbSchID  
  ieee8021BridgeEvbCAPSChannelID  
  ieee8021BridgeEvbCAPAssociateSBPOrURPPort
```

show evb ecp-status

Displays the Edge Control Protocol (ECP) status.

show evb ecp-status [*slot/port*]

Syntax Definitions

slot/port Specifies the switch slot and port number of the chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 6900, 10K

Usage Guidelines

The *slot/port* parameter specifies the port number to display the ECP status. If no port number is specified, then the ECP status is displayed for all the related ports.

Examples

```
-> show evb ecp-status
```

Port	SBP	ACK Timer (msec)	MAX Retry	TX Pkt Counter	TX Retry Counter	TX Fail Counter	Rx Pkt Counter
1/1	10	163.84	3	4	0	0	4
1/1	20	163.84	3	4	0	0	4
1/2	300	163.84	3	5	0	0	5

```
-> show evb ecp-status 1/2
```

Port	SBP	ACK Timer (msec)	MAX Retry	TX Pkt Counter	TX Retry Counter	TX Fail Counter	RX Pkt Counter
0/1/2	300	163.84	3	5	0	0	5

output definitions

Port	Slot and port number of the EVB port.
SBP	ECP port number which is same as SBP number.
ACK Timer	Operational ECP ACK timer in milliseconds.
MAX Retry	Maximum number of retries to receive ACK messages.
TX Pkt Counter	Number of ECP frames transmitted since ECP was instantiated.
TX Retry Counter	Number of times ECP re-tried transmission since ECP was instantiated.

output definitions

TX Fail Counter	Number of times ECP failed to successfully deliver a frame since ECP was instantiated.
RX Pkt Counter	Number of ECP frames received since ECP was instantiated.

Release History

Release 7.3.1; command introduced.

Related Commands

show evb config	Displays the current EVB configuration on the chassis.
evb ecp default-ack-timer	Specifies default wait timer value to receive an acknowledgment (ACK) Edge Control Protocol (ECP) data packet.
evb ecp default-max-retry	Specifies the maximum number of times the ECP must be retransmitted if no ACK - acknowledgment packet is received.

MIB Objects

```

ieee8021BridgeEvbECPTable
  ieee8021BridgeEvbECPPort
  ieee8021BridgeEvbECPOperAckTimerInit
  ieee8021BridgeEvbECPOperMaxRetries
  ieee8021BridgeEvbECPTxFramCount
  ieee8021BridgeEvbECPTxRetryCount
  ieee8021BridgeEvbECPTxFailures
  ieee8021BridgeEvbECPRxFramCount

```

34 Port Mapping Commands

Port Mapping is a security feature that controls communication between peer users. Each session comprises of 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 that is 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 and direction)
port-mapping [unidirectional | bidirectional]
port-mapping unknown-unicast-flooding
show port-mapping status
show port-mapping

port-mapping user-port network-port

Creates a port mapping session with the user ports, network ports, or both user ports and network ports. Use the **no** form of the command to delete ports or a link aggregate group from a session.

port-mapping *port_mapping_sessionid* [**user-port** {*slot slot* | *slot/port[-port2]*} | **linkagg** *linkagg_id*]
[**network-port** {*slot slot* | *slot/port[-port2]*} | **linkagg** *linkagg_id*]

no port-mapping *port_mapping_sessionid* [**user-port** {*slot slot* | *slot/port[-port2]*} | **linkagg** *linkagg_id*]
[**network-port** {*slot slot* | *slot/port[-port2]*} | **linkagg** *linkagg_id*]

Syntax Definitions

<i>port_mapping_sessionid</i>	The port mapping session ID.
user-port	Specifies a user port of the mapping session.
network-port	Specifies a network port of the mapping session.
slot	Specifies that a slot is assigned to the mapping session.
<i>slot</i>	Enter the slot number to be assigned to the mapping session.
<i>port</i>	Enter the port number to be assigned to the mapping session.
<i>port2</i>	Last port number in a range of ports assigned to the mapping session.
linkagg	Specifies that a link aggregation group is assigned to the mapping session.
<i>linkagg_id</i>	Enter a link aggregate ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- User ports that are part of one session cannot communicate with each other. The user ports can communicate only through network ports of the session to the other elements of the system.
- User ports can be part of only one port mapping session.
- 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.

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
-> no port-mapping 5 user-port 2/3
-> no port-mapping 6 network-port linkagg 7
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-mapping	Enables, disables, or deletes a port mapping session.
port-mapping [unidirectional bidirectional]	Configures the direction of a port mapping session.
port-mapping unknown-unicast-flooding	Enables or disables flooding of unknown unicast traffic from all ports to user ports for a particular session.
show port-mapping	Displays the configuration of one or more port mapping sessions.

MIB Objects

```
PortMappingSessionTable
    pmapSessionNumber
portMappingTable
    pmapPortIfindex
    pmapPortType
```

port-mapping

Enables, disables, or deletes a port mapping session.

port-mapping *port_mapping_sessionid* {**enable** | **disable**}

no port-mapping *port_mapping_sessionid*

Syntax Definitions

<i>port_mapping_sessionid</i>	The port mapping session ID.
enable	Enables a port mapping session.
disable	Disables a port mapping session.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command 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 [unidirectional bidirectional]	Configures the direction of a port mapping session.
show port-mapping status	Displays the status of one or more port mapping sessions.
show port-mapping	Displays the configuration of one or more port mapping sessions.

MIB Objects

PortMappingSessionTable
 pmapSessionNumber
 pmapSessionStatus

port-mapping [unidirectional | bidirectional]

Configures the direction of a port mapping session.

port-mapping *port_mapping_sessionid* [**unidirectional** | **bidirectional**]

Syntax Definitions

<i>port_mapping_sessionid</i>	The port mapping session ID.
unidirectional	Specifies unidirectional port mapping.
bidirectional	Specifies bidirectional port mapping.

Defaults

parameter	default
enable disable	enable
unidirectional bidirectional	bidirectional

Platform Supported

OmniSwitch 10K, 6900

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 that is in the unidirectional mode.
- To change the directional mode 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 enable unidirectional
-> port-mapping 5 disable unidirectional
-> port-mapping 6 enable bidirectional
-> port-mapping 5 disable bidirectional
```

Release History

Release 7.1.1; command introduced.

Related Commands

**port-mapping user-port
network-port**

Creates a port mapping session with or without the user ports, network ports or both.

port-mapping

Enables, disables, or deletes a port mapping session.

show port-mapping

Displays the configuration of one or more port mapping sessions.

MIB Objects

PortMappingSessionTable

 PmapSessionNumber

 PmapSessionDirection

port-mapping unknown-unicast-flooding

Enables or disables flooding of unicast traffic from all the switch ports to the user ports related to a particular session.

port-mapping *session_id* unknown-unicast-flooding {enable | disable}

Syntax Definitions

<i>session_id</i>	Enter the port mapping session ID.
enable	Enables the flooding of unknown unicast traffic from all ports to the user ports for a particular session.
disable	Disables the flooding of unknown unicast traffic from all ports to the user ports for a particular session.

Defaults

parameter	default
enable disable	enable

Platform Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Configuring unknown unicast flooding creates a new port mapping session if there is no existing session.
- When a link aggregate is configured as a user port, the unknown unicast flooding configuration is applied to all the member ports of the aggregate.

Examples

```
-> port-mapping 1 unknown-unicast-flooding enable
-> port-mapping 2 unknown-unicast-flooding disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-mapping user-port network-port	Creates a port mapping session with or without the user ports, network ports or both.
port-mapping	Enables, disables, or deletes a port mapping session.
show port-mapping	Displays the configuration of one or more port mapping sessions.
show port-mapping status	Displays the status of one or more port mapping sessions.

MIB Objects

portMappingSessionTable
pmapSessionUnknownUnicastFloodStatus

show port-mapping status

Displays the status of one or more port mapping sessions.

show port-mapping [*port_mapping_sessionid*] **status**

Syntax definitions

port_mapping_sessionid The port mapping session ID.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you do not specify the port mapping session ID, then the status of all the port mapping sessions are displayed.

Examples

-> show port-mapping status

SessionID	Direction	Status	Unknown Unicast
1	bi	enable	drop
2	bi	disable	flood

output definitions

SessionID	Displays the port mapping session ID.
Direction	Displays the direction of a port mapping session.
Status	Displays status of a port mapping session.

Release History

Release 7.1.1; command introduced.

Related Commands

[port-mapping user-port
network-port](#)

Creates a port mapping session with or without the user ports, network ports, or both.

[port-mapping](#)

Enables, disables, or deletes a port mapping session.

MIB Objects

PortMappingSessionTable

PmapSessionNumber

PmapSessionDirection

pmapSessionStatus

show port-mapping

Displays the configuration of one or more port mapping sessions.

show port-mapping [*port_mapping_sessionid*]

Syntax Definitions

port_mapping_sessionid The port mapping session ID.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If you do not specify the port mapping session ID, then the user port and network port information are displayed for all the port mapping sessions active on the switch.

Examples

```
-> show port-mapping 3
```

```

SessionID      USR-PORT      NETWORK-PORT
-----+-----+-----
      1          1/2          1/3
      1          1/6
      1          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 7.1.1; command 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

35 **Learned Port Security Commands**

Learned Port Security (LPS) provides a mechanism for controlling network device communication on one or more switch ports. Configurable LPS parameters allow the user to restrict source learning on a port to:

- A maximum number of learned source MAC addresses.
- A specific amount of time in which source MAC addresses are learned.
- An individual learned source MAC address.
- A range of learned source MAC addresses.

This chapter includes descriptions of the CLI commands used to define LPS parameters and display information about the current LPS configuration.

MIB information for Learned Port Security commands is as follows:

Filename: AlcatelInd1LearnedPortSecurity.mib
Module: ALCATEL-IND1-LPS-MIB

A summary of the available commands is listed here:

port-security
port-security learning-window
port-security convert-to-static
port-security maximum
port-security port max-filtering
port-security mac-range
port-security port violation
port-security learn-trap-threshold
show port-security
show port-security brief
show port-security learning-window

port-security

Enables or disables Learned Port Security (LPS) on the switch port(s). When LPS is enabled, only devices that have a source MAC address that complies with LPS restrictions are learned on the port(s).

port-security {**port** *slot/port*[-*port2*] | **chassis**} **admin-state** {**enable** | **disable** | **locked**}

no port-security **port** *slot/port*[-*port2*]

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
enable	Administratively enables LPS on the specified port(s).
disable	Administratively disables LPS on the specified port(s). All bridged and filtered MAC addresses are cleared, but the static MAC address and LPS configuration for the port is retained. Learning is unrestricted.
locked	Administratively disables all learning on the port. Existing MAC addresses are retained but no additional learning of addresses, except for static MAC addresses, is allowed.

Defaults

By default, LPS functionality is disabled on all ports.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the LPS configuration from the specified port *and* clear all MAC addresses learned on the port. Note that the chassis parameter is not supported when using
- The **admin-state disable** option disables LPS on the port but does not clear the LPS configuration.
- Use the **chassis** parameter to administratively disable or enable all active LPS ports with one command. This option does not apply to ports on which LPS was not previously enabled.
- LPS is supported on Ethernet fixed and 802.1Q-tagged ports.
- LPS is not supported on link aggregates, 802.1Q tagged (trunked) link aggregates, or link aggregate member ports.
- Note that when LPS is enabled on an active port, all MAC addresses previously learned on that port are cleared from the source learning MAC address table.
- LPS is also supported on ports that have Universal Network Profile (UNP) functionality enabled, with the following conditions:
 - When LPS is enabled or disabled on a UNP port, MAC addresses already learned on that port are flushed.

- UNP authentication and classification is applied first, then LPS rules.
- If UNP classifies a MAC address as forwarding but LPS learns the address as filtering, an untagged packet will show as filtering in the default VLAN for the port and a tagged packet MAC will show as filtering in the specific tagged VLAN.
- When a MAC address is filtered by LPS, the **show unp user** command will display “LPS-B” as the classification source for that MAC address.
- LPS allows for the configuration of the following source MAC address learning restrictions:
 - A source learning time limit window to specify the length of time learning is allowed on a port.
 - A maximum number of bridged and filtered MAC addresses allowed on a specific port
 - A list of MAC addresses (individual or range of addresses) allowed on a port.
 - How a port handles traffic that is unauthorized.

Examples

```
-> port-security port 4/8 admin-state enable
-> port-security port 2/1-10 admin-state enable
-> port-security chassis admin-state disable
-> no port-security port 1/1-12
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-security mac-range	Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security learning-window	Configures the amount of time, in minutes, to allow source learning on all LPS ports.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port(s).

MIB Objects

```
learnedPortSecurityTable
  lpsAdminStatus
```

port-security learning-window

Configures the amount of time, in minutes, to allow source learning on all LPS ports. This LPS parameter applies to the entire switch, so when the time limit expires, source learning of *new* MAC addresses is stopped on all LPS ports. Only authorized MAC addresses are allowed to be associated on LPS ports after this timer expires. This command also enables or disables the conversion of dynamic MAC addresses to static MAC addresses on LPS ports.

port-security shutdown *minutes* [**convert-to-static** {**enable** | **disable**}] [**no-aging** {**enable** | **disable**}] [**boot-up** {**enable** | **disable**}]

no port-security learning-window

Syntax Definitions

<i>minutes</i>	The number of minutes during which LPS allows source learning across all LPS ports. This amount of time defines the LPS learning window. The valid range is 1–2880.
convert-to-static enable	Enables the convert-to-static option for the learning window. Dynamically learned bridged (not filtered) MAC addresses are automatically converted to static addresses when the learning window closes.
convert-to-static disable	Disables the convert-to-static option for the learning window. Dynamically learned MAC addresses are not converted to static addresses and will start to age out when the learning window closes.
no-aging enable	Enables the no-aging option for the learning window. Dynamic bridged MAC addresses are learned as <i>pseudo-static</i> MACs, which do not age out but are not saved in the switch configuration.
no-aging disable	Disables the no-aging option for the learning window. MAC addresses are learned as dynamic addresses that will age out.
boot-up enable	Enables the automatic start of the LPS learning window timer when the switch restarts.
boot-up disable	Disables the automatic start of the LPS learning window timer when the switch restarts.

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

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to clear the learning window time (no learning window time limit is applied to the port).
- The LPS source learning time window is started and/or reset each time the **port-security learning-window** command is issued or when the **port-security learning-window boot-up** option is enabled and the switch restarts.
- Even after the LPS learning window time expires, MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of bridged MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.
- If the **no-aging** option is enabled, then all new bridged MAC addresses are learned as pseudo-static MAC addresses during the learning window time period. Pseudo-static addresses do not age out but are not saved to the switch configuration.
- When the **no-aging** option is enabled and the learning window starts, any MAC addresses that were learned prior to the learning window time period are retained as dynamic addresses; they are not converted to pseudo-static MAC addresses.
- If the **convert-to-static** option is enabled, then all dynamic bridged and pseudo-static MAC addresses are converted to static MAC addresses when the learning window closes. Static MAC addresses do not age out and are saved to the switch configuration.

Note. When UNP is enabled on any one LPS port, the **convert-to-static**, **no-aging**, and **boot-up** parameter options are not supported on all LPS-enabled ports. This is because the learning window configuration is global and applies to all LPS ports.

Examples

```
-> port-security learning-window 25
-> port-security learning-window 2 convert-to-static enable
-> port-security learning-window 60 no-aging enable
-> port-security learning-window 500 boot-up disable
-> port-security learning-window 2 convert-to-static enable no-aging enable
-> port-security learning-window 2 no-aging enable convert-to-static enable boot-up
enable
-> no port-security learning-window
```

Release History

Release 7.1.1; command introduced.

Release 7.2.1.R02; **no-aging** and **boot-up** parameters added.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security port max-filtering	Configures the maximum number of MAC addresses that can be filtered on the LPS port.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.
show port-security learning-window	Displays the source learning window configuration.

MIB Objects

```
learnedPortSecurityGlobalGroup  
  lpsLearningWindowTime  
  lpsLearningWindowTimeWithStaticConversion  
  lpsLearningWindowNoAging  
  lpsLearningWindowBootupStatus
```

port-security convert-to-static

Converts all MAC addresses dynamically learned on the LPS port(s) to static MAC addresses. This command does not apply to MAC addresses that are filtered.

port-security {port *slot/port*[-*port2*] | chassis} convert-to-static

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
chassis	Specifies all the LPS ports on the chassis.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Converting dynamic MAC addresses to static MAC addresses is not supported on Universal Network Profile (UNP) ports.
- You can stop the aging out of dynamic MAC addresses on the LPS port(s) by converting them to static MAC addresses.
- The number of converted static MAC addresses cannot exceed the maximum number of MAC addresses allowed on the port(s).

Note. The **port-security convert-to-static** command is not supported on Universal Network Profile (UNP) ports.

Examples

```
-> port-security port 4/8 convert-to-static
-> port-security chassis convert-to-static
```

Release History

Release 7.2.1.R02; command was introduced.

Related Commands**port-security**

Enables or disables Learned Port Security (LPS) on the switch port(s).

port-security maximum

Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

MIB Objects

learnedPortSecurityGlobalGroup

lpsConvertToStatic

port-security maximum

Specifies the maximum number of bridged MAC addresses that an LPS port(s) is allowed to learn.

port-security {**port** *slot/port*[-*port2*]} **maximum** *number*

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>number</i>	The number of source MAC addresses that are allowed on this port. The valid range is 1–1000.

Defaults

By default, the number of MAC addresses allowed is set to 1.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Any additional source MAC addresses received that exceed the maximum number of bridged addresses allowed are filtered on the port, regardless of the LPS learning window time limit. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.
- Note that source learning of configured authorized MAC addresses is still allowed after the LPS time limit has expired; however, all learning is stopped if the number of MAC addresses learned meets or exceeds the maximum number of addresses allowed, even if the LPS time limit has not expired.

Examples

```
-> port-security 2/14 maximum 25
-> port-security 4/10-15 maximum 100
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security learning-window	Configures the amount of time in minutes to allow source learning on all LPS ports.
port-security learn-trap-threshold	Configures the number of bridged MAC addresses to learn before sending a SNMP trap.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

MIB Objects

learnedPortSecurityTable
lpsMaxMacNum

port-security learn-trap-threshold

Configures the number of bridged MAC addresses to learn before sending a SNMP trap.

port-security {**port** *slot/port*[-*port2*]} **learn-trap-threshold** *number*

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>number</i>	The number of bridged MAC addresses to learn before sending a trap. The valid range is 0–1000.

Defaults

By default, the number of bridged MAC addresses to learn before sending a trap is set to the same value as the maximum number of bridged MAC addresses allowed.

Platforms Supported

OmniSwitch 10K, 6900

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.
- If this threshold value is set to zero, a trap is sent for every MAC address learned on the LPS port.

Examples

```
-> port-security port 1/10 learn-trap-threshold 6
-> port-security port 1/10-13 learn-trap-threshold 18
```

Release History

Release 7.1.1; command introduced.

Related Commands**port-security maximum**

Configures the maximum number of source MAC addresses that an LPS port is allowed to learn.

show port-security

Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

learnedPortSecurityTable

lpsLearnTrapThreshold

port-security port max-filtering

Configures the maximum number of MAC addresses that can be filtered on the LPS port(s).

port-security port *slot/port[-port2]* **max-filtering** *number*

Syntax Definitions

<i>slot/port[-port2]</i>	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>number</i>	The maximum number of filtered MAC addresses that are allowed on this port. The valid range is 0–100.

Defaults

By default, the maximum number of MAC addresses that can be filtered on an LPS port is 5.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When the number of filtered MAC addresses learned on the port reaches the maximum, the violation mode (restrict, discard, or shutdown) configured for the port is applied.
- Any additional source MAC addresses received that exceed the maximum number of bridged addresses allowed are filtered on the port, regardless of the LPS learning window time limit. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.
- Even after the LPS learning window time expires, MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.

Examples

```
-> port-security 1/10 max-filtering 6
-> port-security 1/10-13 max-filtering 18
```

Release History

Release 7.1.1; command introduced.

Related Commands

- port-security maximum** Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
- port-security learning-window** Configures the amount of time in minutes to allow source learning on all LPS ports.
- port-security port violation** Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.
- show port-security** Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

learnedPortSecurityTable
lpsMaxFilteredMacNum

port-security mac-range

Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port. This command also enables LPS on the specified port, if LPS is not already active on the port.

port-security {**port** *slot/port*[-*port2*]} **mac-range** [**low** *mac_address* / **high** *mac_address*]

Syntax Definitions

<i>slot/port</i> [- <i>port2</i>]	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
low <i>mac_address</i>	MAC address that defines the low end of a range of MACs (for example, 00:20:95:00:10:2A).
high <i>mac_address</i>	MAC address that defines the high end of a range of MACs (for example, 00:20:95:00:10:2F).

Defaults

parameter	default
high <i>mac_address</i>	ff:ff:ff:ff:ff:ff
low <i>mac_address</i>	00:00:00:00:00:00

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If **low** and **high** end MAC addresses are not specified with this command, then the range is set back to the default range value (00:00:00:00:00:00– ff:ff:ff:ff:ff:ff).
- Source MAC addresses received on an LPS port that fall within the authorized range are allowed on the port. An additional entry is made in the LPS table for each of these learned addresses.
- Any additional source MAC addresses received that do not match the configured authorized addresses are not allowed (filtered) on the port, regardless of the LPS learning window time limit or the maximum number of bridged addresses allowed. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.

Examples

```
-> port-security port 4/20 mac-range low 00:20:95:00:fa:5c
-> port-security port 5/11-15 mac-range low 00:da:95:00:00:10 high
00:da:95:00:00:1f
-> port-security port 5/16-20 mac-range high 00:da:95:00:00:1f
-> port-security port 5/11-15 mac-range
```

Release History

Release 7.1.1; command introduced.

Related Commands

port-security	Enables or disables Learned Port Security (LPS) on the switch port(s).
port-security learning-window	Configures the amount of time in minutes to allow source learning on all LPS ports.
port-security maximum	Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.
port-security port max-filtering	Configures the maximum number of MAC addresses that can be filtered on the LPS port.
port-security port violation	Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.
show port-security	Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

```
learnedPortSecurityTable  
  lpsLoMacRange  
  lpsHiMacRange  
  lpsRowStatus
```

port-security port violation

Selects the method for handling traffic that does not comply with LPS restrictions for the specified port(s).

port-security port *slot/port[-port2]* violation {shutdown | restrict | discard}

Syntax Definitions

<i>slot/port[-port2]</i>	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
shutdown	The port is administratively disabled when the port receives unauthorized traffic. No further traffic is allowed on the port.
restrict	Disables learning on the port when unauthorized traffic is received or the configured maximum number of MAC addresses is reached.
discard	Discards unauthorized traffic but allows traffic that complies with LPS restrictions to forward on the port. The port remains administratively enabled.

Defaults

By default, the security violation mode is set to **restrict** when LPS is enabled on the port.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When a traffic violation occurs on an LPS port, a notice is sent to the switch log.
- If the violation mode is set to **restrict**, unauthorized source MAC addresses are not learned in the LPS table, but they are recorded in the source learning MAC address table with a filtered operational status. This allows the user to view MAC addresses attempting unauthorized access to the LPS port.

Examples

```
-> port-security port 2/14 violation restrict
-> port-security port 4/10-15 violation shutdown
-> port-security port 1/37 violation discard
```

Release History

Release 7.1.1; command introduced.
Release 7.2.1.R02; **discard** parameter added.

Related Commands**port-security**

Enables or disables Learned Port Security (LPS) on the switch port(s).

clear violation

Clears all port violations; allows the port to resume normal operation without a manual reset of the port or module.

show port-security

Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

learnedPortSecurityTable

lpsViolationOption

show port-security

Displays Learned Port Security (LPS) configuration and table entries.

show port-security {**port** [*slot/port*[-*port2*] / **slot** *slot*]}

Syntax Definitions

slot/port[-*port2*] The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

slot Enter the slot number for a module to specify that the command should include all ports on that module (for example, 6 specifies all ports on the module found in slot 6 of the switch chassis).

Defaults

By default, all ports with an LPS configuration are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Displays ports that have an LPS configuration, even if LPS is disabled on the port.
- Use the **port** parameter with this command to display the LPS configuration for a specific port or a range of ports.
- Use the **slot** parameter with this command to display the LPS configuration for all the ports on a specific slot.
- In addition, MAC addresses learned on the LPS enabled port that are within the specified MAC address range appear as a separate entries in the LPS table as dynamic MAC type addresses.
- The MAC Type field is blank if an authorized MAC address range is configured for the LPS port.

Examples

```
-> show port-security port 1/1
```

```
Port: 1/1
Admin-State      :                ENABLED,
Operation Mode   :                ENABLED,
Max MAC bridged  :                3,
Trap Threshold   :                1,
Violation        :                RESTRICT
Max MAC filtered :                5,
Low MAC Range    :                00:00:00:00:00:00,
High MAC Range   :                ff:ff:ff:ff:ff:ff,
Violating MAC    :                NULL
```

MAC	VLAN	MAC TYPE	OPERATION
00:11:22:22:22:21	1	STATIC	bridging

00:11:22:22:22:22	1	STATIC	bridging
00:11:22:22:22:23	1	PSEUDO-STATIC	bridging

output definitions

Port	The module slot number and the physical port number on that module.
Admin-State	The LPS administrative state for the port (Enabled , Disabled , or Locked). Configured through the port-security command.
Operation Mode	The LPS operational mode for the port (Enabled , Disabled , Restricted , Shutdown , Discard , Locked , or Filtered-only).
Max MAC bridged	The maximum number of bridged MAC addresses that are allowed on this port. Configured through the port-security maximum command.
Trap Threshold	The number of bridged MACs to learn before sending a trap. After this number is reached, a trap is sent out for every MAC learned thereafter. If disabled is displayed in this field, the trap threshold is not in force. Configured through the port-security learn-trap-threshold command.
Violation	The security violation mode for the port (restrict , shutdown , or discard). Configured through the port-security port violation command.
Max MAC filtered	The maximum number of filtered MAC addresses that the LPS port can learn. Configured through the port-security port 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.
Violating MAC	The MAC Address that caused the violation on this port.
MAC	The MAC address learned dynamically or configured statically on the LPS port.
VLAN	The VLAN to which the LPS port belongs.
MAC TYPE	Indicates if the MAC address was dynamically learned or statically configured as an authorized MAC address for the port.
OPERATION	The operational status of the MAC address (bridging or filtering).

Release History

Release 7.1.1; command introduced.

Release 7.2.1.R02: **Admin-State** and **Violating MAC** fields added.

Related Commands

[show port-security learning-window](#)

Displays the amount of time during which source learning can occur on all LPS ports.

MIB Objects

learnedPortSecurityTable

- lpsAdminStatus
- lpsOperStatus
- lpsMaxMacNum
- lpsLearnTrapThreshold
- lpsViolationOption
- lpsMaxFilteredMacNum
- lpsLoMacRange
- lpsHiMacRange
- lpsViolatingMac
- lpsRelease

show port-security brief

Displays the LPS port configuration for all the LPS ports.

show port-security brief

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The LPS port parameter values are displayed even if the LPS is disabled on the port.
- The operation mode displayed for the LPS port is based on a combination of the existing admin status and operational status of the port, the result of which is one of the following values:
 - > Enabled
 - > Restricted (only when admin status is enabled)
 - > Shutdown (only when admin status is enabled)
 - > Discard (only when admin status is enabled)
 - > Disabled
 - > Locked
 - > Filtered_only

Examples

-> show port-security brief

Slot/ Port	Operation Mode	Max Bridge	Max Filter	Nb Macs Dyn Br	Nb Macs Dyn Fltr	Nb Macs Static Br	Nb Macs Static Fltr
1/1	ENABLED	5	100	5	10	0	0
1/2	ENABLED	5	100	0	10	5	0
1/3	RESTRICTED	5	100	5	100	0	0
1/4	SHUTDOWN	5	100	-	-	-	0
1/5	DISABLED	5	100	-	-	-	0
1/6	LOCKED	5	100	-	-	3	0

output definitions

Slot/Port	The slot number for the module and the physical port number on that module (e.g., 1/2 specifies port 2 on slot 1).
Operation Mode	Displays the status of the LPS port.
Max Bridge	The maximum number of bridged MAC addresses that are allowed on the LPS 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 port max-filtering command.
Nb Macs Dyn Br	Total number of bridged MAC addresses learned on the LPS port.
Nb Macs Dyn Fltr	Total number of filtered MAC addresses learned on the LPS port.
Nb Macs Static Br	Total number of bridged static MAC addresses (configured static and MAC addresses learned as pseudo-static) on the LPS port.
Nb Macs Static Fltr	Total number of filtered static MAC addresses configured on the LPS port.

Release History

Release 7.2.1.R02; command was introduced.

Related Commands

show port-security Displays the LPS configuration and table entries for individual LPS ports.

MIB Objects

```
learnedPortSecurityTable
  lpsMaxMacNum
  lpsMaxFilteredMacNum
  lpsMaxStaticMacNum
  lpsOperStatus
  lpsAdminStatus
```

show port-security learning-window

Displays the source learning window configuration.

show port-security learning-window

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The source learning time limit is a switch-wide parameter that applies to all ports that have LPS enabled.
- If the learning window time is not set, then no source learning time limit is applied to LPS ports.
- Even after the LPS learning window time expires, dynamic MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of bridged MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.

Examples

```
-> show port-security learning-window
Learning-Window           = 2 min,
Convert-to-static         = DISABLE,
No Aging                  = DISABLE,
Boot Up                   = ENABLE,
Remaining Learning Window = 120 sec
```

output definitions

Learning-Window	The configured amount of time during which the LPS port can learn new MAC addresses.
Convert-to-static	Indicates whether or not dynamic bridged or pseudo-static MACs are converted to static MACs (enabled or disabled).
No Aging	Indicates whether or not bridged MAC addresses are learned as pseudo-static MAC addresses, which don't age out during the LPS learning window time period (disabled or enabled).

output definitions

Boot Up	Indicates whether or not the learning window automatically starts when the switch boots up (enabled or disabled).
Remaining Learning Window	The remaining amount of time during which the LPS port can learn MAC addresses.

Release History

Release 7.1.1; command introduced.

Release 7.2.1.R02; **LPS Shutdown Config** field changed to **Learning-Window, No Aging** and **Boot Up** fields added.

Related Commands

port-security learning-window	Configures the learning window parameters that are applied to all LPS ports.
show port-security	Displays the LPS configuration and table entries for individual LPS ports.

MIB Objects

```
learnedPortSecurityGlobalGroup
  lpsLearningWindowTime
  lpsLearningWindowTimeWithStaticConversion
  lpsLearningWindowNoAging
  lpsLearningWindowBootupStatus
  lpsLearningWindowTimeRemaining
```

36 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 inbound and outbound traffic 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 capture and examine the data traffic to and from a monitored 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 the port to mirror and the port that is to receive data from the mirrored port. Also, enables or disables remote port mirroring.

port-mirroring *port_mirror_sessionid* **source** {*slot/port*[-*port2*] [*slot/port*[-*port2*]...]}
destination *slot/port* [**rpmir-vlan** *vlan_id*] [**bidirectional** | **inport** | **outport**] [**unblocked** *vlan_id*]
[**enable** | **disable**]

port-mirroring *port_mirror_sessionid* **no source** {*slot/port*[-*port2*] [*slot/port*[-*port2*]...]}

Syntax Definitions

<i>port_mirror_sessionid</i>	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.
destination	Specifies the destination port, that receives all the mirrored packets.
<i>slot/port</i>	Enter a port number.
[<i>slot/port</i> [- <i>port2</i>]...]	Enter a range of port numbers.
rpmir-vlan <i>vlan_id</i>	Specifies a reserved VLAN to carry the mirroring traffic.
bidirectional	Specifies bidirectional port mirroring.
inport	Specifies incoming unidirectional port mirroring.
outport	Specifies outgoing unidirectional port mirroring.
unblocked <i>vlan_id</i>	Specifies the VLAN that is to be protected from Spanning Tree changes when port mirroring is active. Ports in this VLAN remain unblocked.
enable	Enables port mirroring status.
disable	Disables port mirroring status.

Defaults

parameter	default
bidirectional inport outport	bidirectional
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You can configure a port mirroring and a port monitoring session on the same network interface module in an OmniSwitch 10K, 6900.
- A mirroring port can not be assigned to a tagged VLAN port.
- When a port is configured as a mirroring port, it does not belong to any VLAN. Inbound traffic to the mirroring port is dropped since it does not belong to any VLAN.
- Spanning tree is disabled by default on a mirroring port.
- Port mirroring is not supported on logical link aggregate ports. However, it is supported on individual ports that are members of a link aggregate.
- Execute the **port mirroring source destination** command to define the mirrored port and enable port mirroring status. Use the **port mirroring** command to enable the port mirroring session.
- Specify the *vlan_id* number of the mirroring port that is to remain **unblocked** when the command is executed. The **unblocked** VLAN becomes the default VLAN for the mirroring port. This VLAN handles the inbound traffic for the mirroring port. Spanning tree remains disabled on the unblocked VLAN.

Usage Guidelines - Remote Port Mirroring

- Remote port mirroring is supported only on OmniSwitch 10K, 6900 switches.
- Use the **rpmir-vlan** parameter and VLAN ID with this command to configure remote port mirroring and to assign the VLAN ID for remote port mirroring.
- The VLAN ID assigned for remote port mirroring cannot be assigned to a general port mirroring port.
- There must not be any physical loop present in the remote port mirroring VLAN.
- Source learning must be disabled or overridden on the ports belonging to the remote port mirroring VLAN on intermediate and destination switches.
- On OmniSwitch 10K, 6900 switches the QoS redirect feature can be used to override source learning.
- The **mac-learning** command can also be used to disable learning on the RPMIR VLAN ID.

Examples

```
-> port-mirroring 6 source 2/2
-> port-mirroring 6 source 2/3-5
-> port-mirroring 6 destination 1/12 rpmir-vlan 7
-> port-mirroring 6 no source 2/2-5

-> port-mirroring 7 source 2/3 destination 6/4 unblocked 750

-> port-mirroring 8 source 1/7 bidirectional
-> port-mirroring 8 no source 1/7

-> port-mirroring 9 source 1/23 inport
-> port-mirroring 9 destination 1/24
-> port-mirroring 9 disable
```

Release History

Release 7.1.1; command 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

mirrorRowStatus

mirrorDirection

mirrorSessOperStatus

mirrorTaggedVLAN

port-mirroring

Enables, disables, or deletes a port mirroring session.

port-mirroring *port_mirror_sessionid* {**enable** | **disable**}

no port-mirroring *port_mirror_sessionid*

Syntax Definitions

port_mirror_sessionid Mirroring session identifier.

enable Enables port mirroring.

disable Disables port mirroring.

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a port mirroring session.
- Use the [port-mirroring source destination](#) command to specify the mirrored ports and destination port. before using this command to enable or disable port mirroring activity for the particular port mirroring session.

Examples

```
-> port-mirroring 6 enable
-> port-mirroring 6 disable
-> no port-mirroring 6
```

Release History

Release 7.1.1; command 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

mirrorTaggedVLAN

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 | output | bidirectional] [timeout seconds] [enable | disable] [capture-type {full | brief}]
```

Syntax Definitions

<i>port_monitor_sessionid</i>	Monitoring session identifier.
<i>slot/port</i>	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).
file filename	Specifies a file name and pathname for capturing information related to the monitoring session (for example, /flash/port2.enc).
<i>filesize</i>	Specifies the size of the file in 64K byte increments. For example, a value of 3 would specify a size of (3 x 64K) bytes.
no file	<i>This option is not supported at this time.</i>
overwrite on	Specifies that capturing of data packets into the port monitoring file continues and old information is overwritten if the total data exceeds the specified file size.
overwrite off	Specifies that capturing of data packets into the port monitoring file is stopped when the maximum file size is reached.
inport	Specifies incoming unidirectional port monitoring.
output	Specifies outgoing unidirectional port monitoring.
<i>seconds</i>	Specifies the number of seconds after which the session is disabled.
enable	Enables the port monitoring status.
disable	Disables the port monitoring status.
full	Captures port monitoring information in detail.
brief	Captures only the concise port monitoring data transmitted.

Defaults

parameter	default
<i>filesize</i>	1
on off	on
bidirectional inport outport	bidirectional
<i>seconds</i>	0
enable disable	disable
capture-type	brief

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You can configure a port mirroring and a port monitoring session on the same NI module in an OmniSwitch 10K, 6900.
- If the port monitoring capture-type is set to **brief**, the first 64 bytes of the traffic is captured. If the port-monitoring capture-type is set to **full**, the entire packet is captured.
- 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.
- The **/flash** directory is the default and the only directory used to capture the port monitoring files.
- The format of the file created is compliant with the ENC file format (Network General Sniffer Network Analyzer Format).
- By default, the recent frames overwrite the 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.

Examples

```
-> port-monitoring 6 source 2/3
-> port-monitoring 6 source 2/3 file /flash/user_port size 2 enable
-> port-monitoring 6 source 2/3 file /flash/user_port capture-type full
```

Release History

Release 7.1.1; command 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
  monitor
  monitorSessionNumber
  monitorIfindex
  monitorFileStatus
  monitorFileName
  monitorFileSize
  monitorScreenStatus
  monitorScreenLine
  monitorCaptureType
  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

<i>port_monitor_sessionid</i>	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 10K, 6900

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 7.1.1; command 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 10K, 6900

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 Destination	Mirror Direction	Unblocked Vlan	Config Status	Oper Status
6.	1/41	-	NONE	Enable	Off
	Mirror Source				
6.	1/20	bidirectional	-	Enable	Off
6.	1/21	bidirectional	-	Enable	Off
6.	1/22	bidirectional	-	Enable	Off
6.	1/23	bidirectional	-	Enable	Off
6.	1/24	bidirectional	-	Enable	Off
6.	1/25	bidirectional	-	Enable	Off
6.	1/26	bidirectional	-	Enable	Off
6.	1/27	bidirectional	-	Enable	Off
6.	1/28	bidirectional	-	Enable	Off
6.	1/29	bidirectional	-	Enable	Off
6.	1/30	bidirectional	-	Enable	Off

output definitions

Session	The port mirroring session identifier.
Mirror Destination	The location of the mirrored port.
Mirror Direction	The direction of the mirroring or mirrored port, which can be bidirectional (the default), inport , or outport .
Unblocked VLAN	The mirroring VLAN ID number.

output definitions (continued)

Config Status	The configuration status of the session.
Oper Status	The current status of the mirroring or mirrored port.
Mirror Source	The location of the mirroring port.

On OmniSwitch 10K, 6900 series switches:

-> show port-mirroring status

Session	Mirror Destination	Mirror Direction	Unblocked Vlan	Config Status	Oper Status
6.	1/41	-	NONE	Enable	Off
	Mirror Source				
6.	1/20	bidirectional	-	Enable	Off
6.	1/21	bidirectional	-	Enable	Off
6.	1/22	bidirectional	-	Enable	Off
6.	1/23	bidirectional	-	Enable	Off
6.	1/24	bidirectional	-	Enable	Off
6.	1/25	bidirectional	-	Enable	Off
6.	1/26	bidirectional	-	Enable	Off
6.	1/27	bidirectional	-	Enable	Off
6.	1/28	bidirectional	-	Enable	Off
6.	1/29	bidirectional	-	Enable	Off
6.	1/30	bidirectional	-	Enable	Off

output definitions

Session	The port mirroring session identifier.
Mirror Destination	The location of the mirrored port.
Mirror Direction	The direction of the mirroring or mirrored port, which can be bidirectional (the default), inport , or outport .
Unblocked VLAN	The mirroring VLAN ID number.
Config Status	The configuration status of the session.
Oper Status	The current status of the mirroring or mirrored port.
Mirror Source	The location of the mirroring port.

Release History

Release 7.1.1; command 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 receives data from the mirrored port, and enables or disables port mirroring status.

MIB Objects

mirrorTable

mirrorMirroringIfindex

mirrorMirroredIfindex

mirrorDirection

mirrorStatus

mirrorSessionNumber

mirrorSessOperStatus

mirrorSrcStatus

mirrorSrcDirection

mirrorSrcRowStatus

mirrorSrcOperStatus

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 10K, 6900

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
```

```

Sess Mon. Mon. Over Oper. Admin Capt. Max. File
      Src Dir write Stat Stat Type Size Name
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
  1.  1/2  Out  OFF  OFF  OFF  Brief   64K  /flash/pm.enc

```

output definitions

Sess	Session - The port monitoring session identifier.
Mon. Src	Monitor Source - The source ports that are monitored.
Mon Dir	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.
Oper Stat	Operating Status - The current operating status of the port monitoring session (on/off).
Admin Stat	Admin Status - The current administrative status of the port monitoring session (on/off).
Capt Type	Capture type - Brief - captures only 64 bytes of data per traffic data packet. Full - captures the entire packet.
Max Size	Maximum Size - The maximum size of the port monitoring file.
File Name	The name of the port monitoring file.

Release History

Release 7.1.1; command 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
  monitorFileStatus
  monitorFileName
  monitorFileSize
  monitorScreenStatus
  monitorScreenLine
  monitorTrafficType
  monitorDirection
  monitorTimeout
  monitorCaptureType
  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

A single line from the captured packet is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Only a single line from the captured packet is displayed, even though the full packet is captured. To view the entire packet, download the file and view it using compatible network analyzer tool.

Examples

```
-> show port-monitoring file 1
```

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 7.1.1; command 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
  monitorFileStatus
  monitorFileName
  monitorFileSize
  monitorScreenStatus
  monitorScreenLine
```

37 sFlow Commands

sFlow is a network monitoring technology that gives visibility in to the activity of the network, by providing network usage information. It provides the data required to effectively control and manage the network usage. sFlow is a sampling technology that meets the requirements for a network traffic monitoring solution.

sFlow provides a network-wide view of usage and active routes. It is used for measuring network traffic, collecting, storing, and analyzing the traffic data. As it is scalable, that doesn't add significant network load. sFlow is an industry standard with many vendors delivering products with this support. Some of the applications of the sFlow data include:

- Detecting, diagnosing, and fixing network problems
- Real-time congestion management
- Detecting unauthorized network activity
- Usage accounting and billing
- Understanding application mix
- Route profiling and peer optimization
- Capacity planning

sFlow is a sampling technology embedded within switches/routers. It provides the ability to monitor the traffic flows. It requires an sFlow agent software process running as part of the switch software and a sFlow collector which receives and analyses the monitored data. The sFlow collector makes use of SNMP to communicate with an sFlow agent in order to configure sFlow monitoring on the device (switch).

An sFlow agent running on the switch/router combines interface counters and traffic flow (packet) samples, preferably, on all the interfaces into sFlow datagrams that are sent across the network to an sFlow collector.

Packet sampling on the switch/router is typically performed by the switching/routing ASICs, providing wire-speed performance. In this case, an sFlow agent does very little processing, by packaging data into sFlow datagrams that are immediately sent on network. This minimizes the memory and CPU utilization by the sFlow agent.

MIB information for the sFlow commands is as follows:

Filename: AlcatelIND1PortMirMon.MIB
Module: Alcatel-IND1-PORT-MIRRORING-MONITORING-MIB

Filename: SFLOW_RFC3176.MIB
Module: SFLOW-MIB

A summary of the available commands is listed here:

sflow agent
sflow agent
sflow sampler
sflow poller
show sflow agent
show sflow receiver
show sflow sampler
show sflow poller

sflow agent

Configures a specific sflow agent IP address.

sflow agent ip <ip_address>

no sflow agent ip <ip_address>

Syntax Definitions

ip_address The sflow agent IP address.

Defaults

parameter	default
<i>ip-address</i>	0.0.0.0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete the IP address.
- If no IP address is configured 0.0.0.0 is used.
- If no IP address is configured but the Loopback0 address is configured, the Loopback0 address is used.

Examples

```
-> sflow agent ip 192.168.1.1  
-> no sflow agent ip 192.168.1.1
```

Release History

Release 7.1.1; command was introduced.

sflow receiver

Sets the destination hosts where the sFlow datagrams are sent out. If there are multiple destinations, then each destination has an instance of the receiver. All these receivers are attached to the sFlow manager instance and to an associated sampler/poller.

sflow receiver *receiver_index* {**name** *string* | **timeout** { *seconds* | **forever** } | **address** {*ip_address* | *ipv6address*} | **udp-port** *port* | **packet-size** *size* **Version** *num* | **release**}

Syntax Definitions

<i>receiver_index</i>	Specifies the receiver index.
<i>string</i>	Specifies the name.
<i>seconds</i> / forever	Specifies the timeout value.
<i>ip_address</i> / <i>ipv6address</i>	Specifies the 32/128-bit ip address.
<i>port</i>	Specifies the UDP (destination) port.
<i>size</i>	Specifies the maximum number of data bytes (size) that can be sent.
<i>num</i>	Specifies the version number.

Defaults

parameter	default
<i>string</i>	empty
<i>seconds</i>	0
<i>ip_address</i>	0.0.0.0(ipv4)
<i>port</i>	6343
<i>size</i>	1400
<i>version num</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **release** form at the end of the command to delete a receiver.

Examples

```
-> sflow receiver 1 name Golden Rcvr1 address 198.206.181.3
-> sflow receiver 1 release
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show sflow receiver Displays the receiver table.

MIB Objects

```
sFlowRcvrTable
  sFlowRcvrIndex
  sFlowRcvrOwner
  sFlowRcvrTimeout
  sFlowRcvrMaximumDatagramSize
  sFlowRcvrAddressType
  sFlowRcvrAddress
  sFlowRcvrPort
  sFlowRcvrDatagramVersion
```

sflow sampler

Gets the hardware sampled from Q-dispatcher and fills up the sampler part of the UDP datagram.

sflow sampler *num* **port** *slot/port[-port]* {**receiver** *receiver_index* | **rate** *value* | **sample-hdr-size** *size*}

no sflow sampler *num portlist*

Syntax Definitions

<i>num</i>	Specifies the instance id.
<i>slot/port</i>	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>receiver_index</i>	Specifies the receiver index.
<i>value</i>	Specifies the rate value for packet sampling.
<i>size</i>	Specifies the maximum number of bytes (size) that can be copied from a sampled packet.
<i>portlist</i>	Specifies the interface index range.

Defaults

parameter	default
<i>receiver_index</i>	0
<i>value</i>	0
<i>size</i>	128

Platforms Supported

OmniSwitch 10K, 6900

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 receiver 1 rate 5 sample-hdr-size 64
-> no sflow sampler 1 2/1-5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show sflow sampler Displays the sampler table.

MIB Objects

sFlowFsTable
 sFlowFsDataSource
 sFlowFsInstance
 sFlowFsReceiver
 sFlowFsPacketSamplingRate
 sFlowFsMaximumHeaderSize

sflow poller

Gets counter samples from ethernet driver and fills up the counter part of the UDP datagram.

sflow poller *num port slot/port[-port] {receiver receiver_index | interval value}*

no sflow poller *num portlist*

Syntax Definitions

<i>num</i>	Specifies the instance id.
<i>slot/port</i>	The slot number for the module and the physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
<i>receiver_index</i>	Specifies the receiver index.
<i>value</i>	Specifies the maximum number of seconds between successive samples (interval value).
<i>portlist</i>	Specifies the interface index range.

Defaults

parameter	default
<i>receiver_index</i>	0
<i>value</i>	0

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **no** form of this command to delete a poller.

Examples

```
-> sflow poller 1 1/1 receiver 2 interval 20
-> sflow poller 1 2/6-10 receiver 1 interval 30
-> no sflow poller 1 2/6-10
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show sflow poller](#) Displays the poller table.

MIB Objects

sFlowCpTable

sFlowCpDataSource

sFlowCpInstance

sFlowCpReceiver

 sFlowCpInterval

show sflow agent

Displays the sflow agent table.

show sflow agent

Syntax Definitions

agent Collects sample datagrams and send it to the collector across the network.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- It is necessary to execute the **ip interface** command to make a loopback0 IP address as the fixed primary address of the switch, in order to avoid interface changes, which might need the collector software to be restarted for it to communicate using the new agent IP address. Normally, the primary IP address could change depending on the IP interface going up/down. Therefore, the sFlow agent always needs to send a fixed IP address in the datagram.
- The loopback address should be an IP interface configured on the switch.

Examples

```
-> ip interface loopback0 address 198.206.181.100
-> show sflow agent
Agent Version = 1.3; Alcatel-Lucent; 6.1.1
Agent IP      = 127.0.0.1
```

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 7.1.1; command was introduced.

Related Commands

show sflow receiver Displays the receiver table.

MIB Objects

sFlowAgent

sFlowVersion

sFlowAgentAddressType

 sFlowAgentAddress

show sflow receiver

Displays the sflow receiver table.

show sflow receiver [*num*]

Syntax Definitions

num Specifies the receiver index.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands**sflow agent**

Sets the destination hosts where the sFlow datagrams are sent out.

MIB Objects

sFlowRcvrTable

sFlowRcvrIndex

show sflow sampler

Displays the sflow sampler table.

show sflow sampler*[num]*

Syntax Definitions

num Specifies the instance id.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands**sflow sampler**

Gets hardware sampled from Q-dispatcher.

MIB Objects

sFlowFsTable

 sFlowFsInstance

show sflow poller

Displays the sflow poller table.

show sflow poller [*num*]

Syntax Definitions

num Specifies the instance id.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands**sflow poller**

Gets counter samples.

MIB Objects

sFlowCpTable

sFlowCpInstance

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.
<i>entry-number</i>	The entry number in the list of probes (<i>optional</i>).
enable	Enables the RMON probe.
disable	Disables the RMON probe.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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.
<i>entry-number</i>	The entry number in the list of probes (<i>optional</i>).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

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 7.1.1; 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 Switch Logging Commands

This chapter includes descriptions for Switch Logging commands. These commands are used to configure parameters for the Switch Logging utility.

MIB information for the system commands is as follows:

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

A summary of the available commands is listed here.

swlog
swlog appid
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 {[enable | disable] | remote command-log {enable| disable} | preamble | hash-time-limit *num* | duplicate-detect | console level *num*}

no swlog

Syntax Definitions

enable disable	Enables or disables the switch logging functionality.
command-log enable disable	Enables or disables the logging of commands to syslog.
preamble	Enables or disables the display of the preamble to the console.
hash-time-limit <i>num</i>	Configures the amount of elapsed time for an entry to no longer be considered a duplicate entry.
duplicate-detect	Enables or disables the duplicate detection capability.
level <i>num</i>	The severity level filter keyword or numeric value for the application ID. (see table for swlog appid command).

Defaults

By default, switch logging is enabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of the command to enable or disable the **preamble** and **duplicate-detect** setting.
- The syslog preamble includes the level, appid and timestamp that precedes the actual log messages.
- If duplicate entries are received within the configured **hash-time-limit** only a single entry will be logged along with the number of times duplicated.

Examples

```
-> swlog enable
-> swlog hash-time-limit 30
-> no swlog preamble
```

Release History

Release 7.1.1; command was introduced.

Related Commands

swlog appid	Defines the level at which switch logging information will be filtered for the specified application.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

systemSwitchLoggingGroup
 systemSwitchLoggingEnable

swlog appid

Defines the level at which switch logging information will be filtered for the specified application. All application events of the defined level and lower are captured.

```
swlog appid {all | string} {[library {all | string} | subapp {all | num}]} {[disable | enable | level {level | num}]} [vrf num]
```

Syntax Definitions

<i>string</i>	An application or library identification keyword.
subapp <i>num</i>	A numerical equivalent value for the subapp ID.
disable enable	Enables or disables the logging of the associated application.
level <i>level</i> <i>num</i>	The severity level filter keyword or numerical equivalent value for the application ID (<i>see table below</i>). All switch logging messages of the specified level and lower will be captured. The severity level is a value assigned to the relative severity of the switch logging message. A lower value indicates messages that are more severe, a higher value indicates messages that are less severe.
vrf <i>num</i>	The VRF ID.

Supported Levels	Numeric Equivalents	Description
off	0	Disabled
alarm	1	Highest severity. The system is about to crash and reboot.
error	2	System functionality is reduced.
alert	3	A violation has occurred.
warning	4	A unexpected, non-critical event has occurred.
info	5	Any other non-debug message (default).
debug1	6	A normal event debug message.
debug2	7	A debug-specific message.
debug3	8	All debug messages.

Defaults

Default severity level is **info**.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **show swlog appid all** command to display all available registered applications.

Examples

```
-> swlog appid all subid all enable
-> swlog appid mvrpNi subapp 1 level 8
-> show swlog appid mvrpNi
```

```
Application Name           : mvrpNi,
```

SubAppl ID	Sub Application Name	Level	VRF	Level
1	main	error	VRF	1-64 info

Release History

Release 7.1.1; command was introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
  systemSwitchLoggingLevelAppName
  systemSwitchLoggingLevel
  systemSwitchLoggingVrf
```

swlog output

Enables or disables switch logging output to the console, file, or data socket (remote session).

swlog output {**tty** {**enable** | **disable**} | **console** | **flash** | **socket** *ip_address* [**vrf-name** *name*]}

no swlog output {**console** | **flash** | **socket** *ip_address*}

Syntax Definitions

tty enable disable	Enables or disables switch logging to a connected Telnet session.
console	Specifies console output. When enabled, switch logging output is printed to the user console.
flash	Specifies /flash file output. When enabled, switch logging output is printed to a file in the switch's /flash file system.
socket	Specifies data socket output. When enabled, switch logging output is printed to a remote session.
<i>ip_address</i>	The IPv4 or IPv6 address for the remote session host.
<i>name</i>	Specifies the VRF to be used to access the remote syslog server.

Defaults

parameter	default
console flash socket	flash and console

Platforms Supported

OmniSwitch 10K, 6900

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 output to a single host using the **socket** keyword, followed by the IP address of the remote host.
- VRF name must either be 'default' or pre-defined VRF (user-defined).

Examples

```
-> swlog output console
-> no swlog output flash
-> swlog output socket 14.1.1.1
-> swlog output socket 14.1.1.1 vrf-name vrf1
```

Release History

Release 7.1.1; command was introduced.

Release 7.3.1; **vrf-name** parameter added.

Related Commands

swlog	Enables or disables switch logging.
swlog appid	Defines the level at which switch logging information will be filtered for the specified application.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup
  systemSwitchLoggingFlash
  systemSwitchLoggingSocket
  systemSwitchLoggingSocketIpAddr
  systemSwitchLoggingConsole
systemSwitchLoggingHostTable
  systemSwitchLoggingHostIpAddr
  systemSwitchLoggingHostPort
  systemSwitchLoggingHostStatus
  systemSwitchLoggingHostVrfName
```

swlog output flash-file-size

Configures the size of the switch logging file.

swlog output flash-file-size *kilobytes*

Syntax Definitions

kilobytes The size of the switch logging file in kilobytes.

Defaults

parameter	default
<i>kilobytes</i>	125

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the [show hardware-info](#) 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 256
```

Release History

Release 7.1.1; command was introduced.

Related Commands

swlog clear	Clears the files that store switch logging data.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

systemSwitchLoggingGroup
 systemSwitchLoggingFileSize

swlog clear

Clears the files that store switch logging data.

swlog clear

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.
show swlog	Displays switch logging information.

MIB Objects

```
systemSwitchLoggingGroup  
  systemSwitchLoggingClear
```

show log swlog

Displays stored switch logging information.

show log swlog

show log swlog [timestamp *mm/dd/yyyy hh:mm:ss*] [slot *num*]

Syntax Definitions

<i>num</i>	The slot number to display the logging information for. Currently not supported.
<i>start_time</i>	Specify the starting time for the switch logging information to be displayed. Use the format <i>mm/dd/yyyy hh:mm:ss</i> where <i>mm</i> represents the month, <i>dd</i> is the day, <i>yyyy</i> is the year, <i>hh</i> is the hour, <i>mm</i> is the minutes and <i>ss</i> is the seconds. Use four digits to specify the year.

Default

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When the switch logging display is too long, you may use the **swlog clear** command to clear all of the switch logging information.
- The use of **grep** and the **timestamp** parameter can be used to filter the log files.

Examples

```
-> show log swlog timestamp 09/30/2011 13:27:00
Displaying file contents for '/flash/swlog.6'
Displaying file contents for '/flash/swlog.5'
<output truncated>
```

```
Sep 30 13:27:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!
```

```
-> show log swlog | grep ChassisSupervisor
Displaying file contents for '/flash/swlog.6'
Displaying file contents for '/flash/swlog.5'
<output truncated>
```

```
Sep 28 13:25:15 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!
```

```
Sep 30 13:26:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!
```

```
Sep 30 13:27:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr
info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!
```


Release History

Release 7.1.1; command was introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid	Adds or removes a filter level for a specified subsystem.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
swlog clear	Clears the files that store switch logging data.
show swlog	Displays switch logging information.

show swlog

Displays switch logging information (e.g., switch logging status, log devices, application IDs with non-default severity level settings).

```
show swlog [library | appid {all | string}]
```

Syntax Definitions

library	The slot number to display the logging information for. Currently not supported.
<i>string</i>	The name of the appid to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command can also be used on the secondary CMM.

Examples

```
-> show swlog
Operational Status           : Running,
File Size per file           : 125K bytes,
Log Device                   : console flash socket,
Log Device                   : ipaddr 1.2.3.4 vrf mgt(1),
Syslog FacilityID           : local0(16),
Remote command-log          : Disabled,
Hash Table entries age limit : 60 seconds,
Switch Log Preamble         : Enabled,
Switch Log Debug             : Disabled,
Switch Log Duplicate Detection : Enabled,
Console Display Level       : info
```

output definitions

Application ID	The Application ID (subsystem) for which the Severity Level is not set to the info (6) default setting.
Operational Status	Displays wheter switch logging is enabled or disabled.
File Size per file	The maximum file size of the switch log file.
Log Device	Which devices are the switch log messages being sent to.
Log Device	Which devices are the switch log messages being sent to.
Syslog FacilityID	Syslog FacilityID
Remote command-log	Status of remote command logging.
Hash Tables entries age limit	The elapsed time for duplicate entries.
Switch Log Preamble	Status of displaying message preamble on console.
Switch Log Debug	Status of swlog debug.
Switch Log Duplicate Detection	Status of duplicate detection.
Console Display Level	The console severity level of the above-referenced Application ID.

Release History

Release 7.1.1; command was introduced.

Related Commands

swlog	Enables or disables switch logging.
swlog appid	Defines the level at which switch logging information will be filtered for the specified application.
swlog output	Enables or disables switch logging output to the console, file, or data socket.
show log swlog	Displays stored switch logging information from flash.

MIB Objects

systemSwitchLoggingHostVrfName

40 Health Monitoring Commands

The Health Monitoring function monitors the consumable resources of the switch (for example, bandwidth usage, CPU usage) and provides a single integrated resource for a Network Management System (NMS). This function monitors the switch, and at fixed intervals, collects the current values for each resource being monitored. Users specify resource threshold limits and traps are sent to an NMS if a value falls above or below a user-specified threshold.

The Health Monitoring commands comply with RFC1212.

MIB information for the Health Monitoring commands is as follows:

Filename: AlcatelIND1Health.mib
Module: healthMIB

A summary of the available commands is listed here:

health threshold
health interval
show health configuration
show health
show health all

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* }

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.
<i>percent</i>	The new threshold value, in percent, for the corresponding resource— rx , txrx , memory , cpu —(0–100).
<i>degrees</i>	The new threshold value, in Celsius, for the chassis temperature threshold (0–100).

Defaults

parameter	default
<i>percentage</i>	80
<i>degrees</i>	50

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When a resource falls back below the configured threshold, an additional trap is sent to the user. This indicates that the resource is no longer operating beyond its configured threshold limit.
- Changing a threshold value sets the value for all levels of the switch (the switch, module, and port). You cannot set different threshold values for each level.
- For detailed information on each threshold type, refer to [page 40-5](#), or refer to the chapter titled “Diagnosing Switch Problems” in your Network Configuration Guide.
- To view the current health threshold values, use the [show health configuration](#) command.

Examples

```
-> health threshold rx 85
-> health threshold txrx 55
-> health threshold memory 95
-> health threshold cpu 85
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show health configuration](#) Displays the current health threshold settings.

MIB Objects

```
HealthThreshInfo
  healthThreshDeviceRxLimit
  healthThreshDeviceTxRxLimit
  healthThreshDeviceMemoryLimit
  healthThreshDeviceCpuLimit
```

health interval

Configures the sampling interval between health statistics checks. The sampling interval is the time interval between polls of the consumable resources of the switch 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
<i>seconds</i>	5

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Decreasing the polling interval may impact switch performance.

Examples

```
-> health interval 6
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show health](#) Displays the current health sampling interval.

MIB Objects

HealthThreshInfo
healthSamplingInterval

show health configuration

Displays current health configuration settings.

show health configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show health configuration
Rx Threshold           : 80
TxRx Threshold        : 80
Cpu Threshold         : 80
Memory Threshold      : 80
Sampling Interval (Secs) : 10
```

output definitions

Rx Threshold	The current device input (RX) threshold. This value displays the maximum percentage of total bandwidth allowed for <i>incoming traffic</i> 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 using 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 <i>all incoming and outgoing traffic</i> . 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 using 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 using 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 using the health threshold command.
Sampling Interval	Displays the sampling interval time period in seconds. The default value is 5 seconds. Sampling interval can be changed using the health interval command.

Release History

Release 7.1.1; command introduced.

Related Commands

health threshold	Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, CPU usage, and chassis temperature.
health interval	Configures the sampling interval between health statistics checks.

MIB Objects

```
HealthThreshInfo
  healthThreshDeviceRxLimit
  healthThreshDeviceTxRxLimit
  healthThreshDeviceTempLimit
  healthThreshDeviceMemoryLimit
  healthThreshDeviceCpuLimit
```

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 [**port** *slot/port* | **slot** *slot* [-*slot1*]] [**statistics**]

Syntax Definitions

port	To view a specific port, enter the slot and port number (for example, 3/1).
slot	To view a series of slots, enter the range of slot numbers (for example, 1-10) along with the slot keyword.
statistics	Optional command syntax. It displays the same information as the show health command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If no slot or port information is specified, the aggregate health statistics for all ports is displayed.

Examples

```
-> show health
```

```

CMM                Current    1 Min    1 Hr    1 Day
Resources          Avg      Avg      Avg      Avg
-----+-----+-----+-----+-----
CPU                0         0         0         0
Memory             30        30        24        24
Receive            01         01         01         01
Transmit/Receive   01         01         01         01
Memory             66         66         66         66
Temperature Cmm    33         33         33         33
Temperature Cmm Cpu 32         32         32         32

```

```
-> show health port 4/3
```

```

Port 04/03
Resources      Limit  Curr    1 Min    1 Hr    1 Hr
              Avg      Avg      Avg      Avg      Max
-----+-----+-----+-----+-----+-----
Receive       80     01     01     01     01
Transmit/Receive 80     01     01     01     01

```

Receive	Traffic received by the switch.
Transmit/Receive	Traffic transmitted and received by the switch.
Memory	Switch memory.
CPU	Switch CPU.
Temperature Cmm	CMM Chassis Temperature.
Temperature Cmm Cpu	CMM CPU Temperature.
Limit	Currently configured device threshold levels (percentage of total available bandwidth or temperature measured in degrees Celsius).
Curr	Current device bandwidth usage or temperature (measured in degrees Celsius).
1 Min Avg	Average device bandwidth usage or temperature (measured in degrees Celsius) over a 1-minute period.
1 Hr Avg	Average device bandwidth usage or temperature (measured in degrees Celsius) over a 1-hour period.
1 Hr Max	Maximum device bandwidth usage or temperature (measured in degrees Celsius) over a 1-hour period (the maximum of the 1 minute averages).

Release History

Release 7.1.1; command introduced.

Related Commands

[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 <i>received</i> on all active NI modules.
txrx	Displays the health statistics for traffic both <i>transmitted and received</i> on all active NI modules.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show health all memory
```

```
* - current value exceeds threshold
```

Memory	Limit	Curr	1 Min Avg	1 Hr Avg	1 Hr 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, TXX, 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 using the health threshold command.
Curr	Current usage of the resource on the corresponding slot, in percent (the amount of the total resource bandwidth actually being used by the 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 7.1.1; command 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
```

41 Ethernet OAM Commands

Service provider networks are large and complex with a wide user base, and they often involve different operators that must work together in order to provide end-to-end services to enterprise customers. Operations, Administration, and Maintenance (OAM) provides service assurance over a converged network that service providers are looking for in an Ethernet network. Ethernet OAM addresses areas such as availability, mean time to repair and more. Ethernet OAM focuses on two main areas that are most in need by service providers and are rapidly evolving in the standards bodies, Service OAM and Link OAM. These two OAM protocols have unique objectives but are complementary to each other. Service OAM provides monitoring and troubleshooting of end-to-end Ethernet service instances, while Link OAM allows a provider to monitor and troubleshoot an individual Ethernet link.

MIB information for the Ethernet OAM commands is as follows:

Filename: AlcatelIND1Eoam.MIB
Module: Alcatel-IND1-ETHERNET-OAM-MIB

Filename: IETF_802_1ag.MI
Module: IEEE8021-CFM-MIB

A summary of the available commands is listed here:

EthOAM vlan Configuration Commands	ethoam vlan
EthOAM Domain Configuration Commands	ethoam domain ethoam domain mhf ethoam domain id-permission
EthOAM Management Association Configuration Commands	ethoam association ethoam association mhf ethoam association id-permission ethoam association ccm-interval ethoam association endpoint-list clear ethoam statistics
EthOAM Default-Domain Configuration Commands	ethoam default-domain level ethoam default-domain mhf ethoam default-domain id-permission ethoam default-domain primary-vlan
EthOAM Management Point Configuration Commands	ethoam endpoint ethoam endpoint admin-state ethoam endpoint rfp ethoam endpoint ccm ethoam endpoint priority ethoam endpoint lowest-priority-defect

EthOAM Loopback and Linktrace Commands	ethoam linktrace ethoam loopback
EthOAM Timer Configuration Commands	ethoam fault-alarm-time ethoam fault-reset-time
EthOAM Performance Monitoring Configuration Commands	ethoam one-way-delay ethoam two-way-delay clear ethoam
EthOAM Show Commands	show ethoam show ethoam domain show ethoam domain association show ethoam domain association end-point show ethoam default-domain configuration show ethoam default-domain show ethoam remote-endpoint domain show ethoam cfmstack show ethoam linktrace-reply show ethoam linktrace-tran-id show ethoam vlan show ethoam statistics show ethoam config-error show ethoam one-way-delay show ethoam two-way-delay

ethoam vlan

Creates an association between Primary VID and Non-Primary VID(s).

ethoam vlan {*vlanid-list*} **primary-vlan** {*vlan-id*}

no ethoam vlan {*vlanid-list*}

Syntax Definitions

vlanid-list VLAN Identifier List e.g. '10 30-40' or '10'

vlan-id VLAN Identifier e.g. '20'

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Each VLAN ID specified must be created before creating any association.
- Each VLAN ID specified must be between 1 and 4094.
- Each VLAN ID specified must be static.
- A Non-Primary VID can only be associated with single Primary VID only.
- Once Primary VID is associated with Non-Primary VID, then it can not be configured as Non-Primary VID. Its association must be removed before it is configured as Non-Primary VID.
- This CLI shall trigger Automip for this VLAN, if either 'mhf' is enabled for MA or default-MD with primary VLAN same as the primary VLAN of this VLAN.
- If the VLAN is deleted using VLAN CLI (no vlan <vid>) and VLAN is non-primary, then the entry for this VLAN in the VLAN table will be deleted. This shall in turn delete all MEPs and MIPs associated with it. If the deleted VLAN is primary VLAN, then all its associated VLAN entries in the VLAN table shall be deleted. This shall in turn delete all MAs on this deleted VLAN.
- Use the **no** form of this command to dissociate Primary VID from the Non-Primary VID(s).

Examples

```
-> ethoam vlan 10 primary-vlan 20
-> ethoam vlan 11-15 primary-vlan 20
-> ethoam vlan 30 40-50 primary-vlan 20
-> no ethoam vlan 10
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam vlan](#)

Displays the Ethernet OAM statistics of all the Management Domains configured on the bridge.

MIB Objects

```
dot1agCfmVlanTable  
  dot1agCfmVlanComponentId  
  dot1agCfmVlanVid  
  dot1agCfmVlanPrimaryVid  
  dot1agCfmVlanRowStatus
```

ethoam domain

Creates an Ethernet domain with a specific name.

ethoam domain *name* **format** {**none** | **dnsname** | **mac-address-uint** | **string**}
level *num*

no ethoam domain *name*

Syntax Definitions

<i>name</i>	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-uint	MAC address + 2-octet (unsigned) integer.
dnsname	Domain Name like string, globally unique text string derived from a DNS name.
<i>num</i>	MD Level and it ranges from 0 to 7

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.3.1; command was introduced.

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 Message Handling Function (MHF) value for MD entry.

ethoam domain *name* **mhf** {**none** | **explicit** | **default**}

Syntax Definitions

<i>name</i>	Specifies the domain name used while creating the management domain for which this management association is created.
none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.

Defaults

parameter	default
none explicit default	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Domain must be created before it is modified.

Examples

```
-> ethoam domain MD mhf default
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam Displays the information of all the Management Domains (MD) configured on the bridge.

MIB Objects

```
dotlagCfmMdTable
  dotlagCfmMdName
  dotlagCfmMdMhfCreation
```

ethoam domain id-permission

Configures the ID-permission value for MD entry.

ethoam domain *name* **id-permission** {*none* | *chassisid*}

Syntax Definitions

<i>name</i>	Specifies the domain name used while creating the management domain for which this management association is created.
none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present. System name shall be filled as Chassis ID.

Defaults

parameter	default
none chassisid	none

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Domain must be created before it is modified.

Examples

```
-> ethoam domain MD id-permission chassisid
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam default-domain configuration	Displays the values of scalar Default-MD objects.
show ethoam domain	Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dotlagCfmMdTable
  dotlagCfmMdName
  dotlagCfmMdIdPermission
```

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

<i>ma_name</i>	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.
<i>md_name</i>	Specifies the domain name used while creating the management domain for which this management association is created.
<i>vlan-id</i>	Primary VLAN Identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.3.1; command was introduced.

Related Commands

[show ethoam domain association](#)

Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

```
dotlagCfmMaNetTable
  dotlagCfmMaNetFormat
  dotlagCfmMaNetName
  dotlagCfmMaNetRowStatus
dotlagCfmMaCompTable
  dotlagCfmMaComponentId
  dotlagCfmMaCompPrimaryVid
  dotlagCfmMaCompRowStatus
```

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

<i>ma_name</i>	Association name for the created Ethernet OAM Association.
<i>md_name</i>	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 10K, 6900

Usage Guidelines

- MA must be created before it is modified.
- On modification of 'mhf' for any MA, Automip shall also be invoked for all VLANS associated with this primary VID.

Examples

```
-> ethoam association MA domain MD mhf-creation defer
```

Release History

Release 7.3.1; command was introduced.

Related Commands

**show ethoam domain
association**

Displays the information of a specified MA in a Management Domain configured on the bridge.

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* *md_name* **id-permission** {**none** | **chassisid** | **defer**}

Syntax Definitions

<i>ma_name</i>	Association name for the created Ethernet OAM Association.
<i>md_name</i>	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 10K, 6900

Usage Guidelines

- MA must be created before it is modified.

Examples

```
-> ethoam association MA domain MD id-permission defer
```

Release History

Release 7.3.1; command was introduced.

Related Commands

**show ethoam domain
association**

Displays the information of a specified MA in a Management Domain configured on the bridge.

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

<i>ma_name</i>	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
<i>md_name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain command on page 41-5 .
interval-invalid	Specifies that no CCMs are sent by a MEP
interval100ms	Specifies the CCMs are sent every 100 milli seconds.
interval1s	Specifies that CCMs are sent every 1 second.
interval10s	Specifies that CCMs are sent every 10 seconds.
interval1m	Specifies that CCMs are sent every minute.
interval10m	Specifies that CCMs are sent every 10 minutes.

Defaults

parameter	default
interval-invalid interval100ms interval1s interval10s interval1m interval10m	interval10s

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The *ma_name* should be unique amid all those used by or available to the service provider within a domain.

Examples

```
-> ethoam association MA domain MD ccm-interval interval10s
```

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain

Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

```
dotlagCfmMaNetTable  
    dotlagCfmMaNetName  
dotlagCfmMaCompTable  
    dotlagCfmMaCompMIdPermission
```

ethoam association endpoint-list

Modifies the MEP list of an Ethernet OAM Maintenance Association.

```
ethoam association ma_name domain {md_name | mac_add}  
endpoint-list mep_id[-mep_id2]
```

```
no ethoam association association_name domain {domain_name | mac_add}  
endpoint-list mep_id[-mep_id2]
```

Syntax Definitions

<i>ma_name</i>	Name of the Ethernet OAM Association. Up to 48 (minus domain name length) characters may be used.
<i>md_name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain command on page 41-5
<i>mac_add</i>	Specifies the CFM system MAC address.
<i>mep_id</i>	Specifies the MEP number.
<i>mep_id2</i>	Last MEP number in a range of MEPs you want to configure.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the MEP list.
- Note that only the MEP that is associated with the MEP list of the MA can be configured locally on the bridge or monitored remotely.
- The *ma_name* should be unique within a domain.

Examples

```
-> ethoam association MA domain MD endpoint-list 100-200  
-> no ethoam association MA domain MD endpoint-list 100-200
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain association](#)

Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

```
dotlagCfmMdTable
  dotlagCfmMdName
dotlagCfmMaNetTable
  dotlagCfmMaNetName
DotlagCfmMaMepList
  dotlagCfmMaMepListIdentifier
  dotlagCfmMaMepListRowStatus
```

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

<i>domain</i>	Specifies the domain name used while creating the management domain for which this management association is created.
<i>association</i>	Association name for the created Ethernet OAM Association.
<i>mep-id</i>	MEP Identifier. Valid Range is 1-8191.

Defaults

None

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

None

Examples

```
-> clear ethoam statistics
-> clear ethoam statistics domain MD association MA endpoint 10
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam statistics](#) Displays the Ethernet OAM of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

MIB Objects

```
dotlagCfmMdTable
    dotlagCfmMdName
dotlagCfmMaNetTable
    dotlagCfmMaNetName
dotlagCfmMepTable
    dotlagCfmMepIdentifier
    alaCfmMepClearStats
    alaCfmGlobalClearStats
```

ethoam default-domain level

Configure the effective level of all default domain entries with the level value set to **no level**.

ethoam default-domain level *{num}*

no ethoam default-domain

Syntax Definitions

num The MD level whose value range from 0-7.

Defaults

Default value is 0.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- MD Level shall range from 0 to 7.

Examples

```
-> ethoam default-domain level 1
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam default-domain configuration](#) Displays the values of scalar Default-MD objects.

MIB Objects

Dot1agCfmDefaultMdLevel

ethoam default-domain mhf

Configure the effective MHF value for all default domain entries with MHF value set to **defer**.

```
ethoam default-domain mhf {none | default | explicit}
```

```
no ethoam default-domain
```

Syntax Definitions

none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level. Defaults

Defaults

Default value is none.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ethoam default-domain mhf default
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam default-domain configuration](#) Displays the values of scalar Default-MD objects.

MIB Objects

```
dot1agCfmDefaultMdDefMhfCreation
```

ethoam default-domain id-permission

Configures the effective ID permission value for all default domain entries with the ID permission value set to **defer**.

ethoam default-domain id-permission {none | chassisid}

no ethoam default-domain

Syntax Definitions

none

Sender ID TLV is not to be sent.

chassisid

Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.

Defaults

Default value is none.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ethoam default-domain id-permission chassisid
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam default-domain configuration](#) Displays the default domain configuration.

MIB Objects

dot1agCfmDefaultMdDefIdPermission

ethoam default-domain primary-vlan

Configures the default domain settings for the specified primary VLAN.

ethoam default-domain primary-vlan {*vlan-id*} [level {no-level | *num*}] [mhf {none | default | explicit | defer}] [id-permission {none | chassisid | defer}]

no ethoam default-domain

Syntax Definitions

<i>vlan-id</i>	VLAN Identifier.
no-level	MD level is inherited from the default domain level.
<i>num</i>	MD Level. Valid range is 0 to 7.
none	No MHFs can be created.
default	MHFs can be created.
explicit	MHFs can be created only if a MEP is created at some lower MD Level.
defer	MHF defers to the default domain MHF value.
none	Sender ID TLV is not to be sent.
chassisid	Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.
defer	ID permission defers to the default domain ID permission value.

Defaults

parameter	default
no-level / <i>num</i>	no-level
none explicit default defer	defer
none chassisid defer	defer

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

On modification of MHF for any primary VID, Automip is invoked for all VLANS associated with this primary VID.

Examples

```
-> ethoam default-domain primary-vlan 10 id-permission chassisid level 3 mhf default.  
-> ethoam default-domain primary-vlan 10 id-permission chassisid  
-> 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 7.3.1; command was introduced..

Related Commands

[show ethoam default-domain](#) Displays the information of all the default MD.

MIB Objects

```
dot1agCfmDefaultMdTable  
  dot1agCfmDefaultMdComponentId  
  dot1agCfmDefaultMdPrimaryVid  
  dot1agCfmDefaultMdLevel
```

ethoam endpoint

Creates a Maintenance End Point (MEP) and virtual MEP.

ethoam endpoint *mep-id* **domain** *md_name* **association** *ma_name* **direction** { **up** | **down** } {**port** {*slot/*
port | **virtual** | **linkagg** *agg_id*} [**primary-vlan** *vlan_id*]

no ethoam endpoint *mep-id* **domain** *md_name* **association** *ma_name*

Syntax Definitions

<i>mep_id</i>	Specifies the Maintenance Association End Point. The valid range is 1–8191.
<i>md_name</i>	Specifies the domain name used while creating the management domain for which this management association is created.
<i>ma_name</i>	Association name for the created Ethernet OAM Association.
up	For UP MEP.
down	For DOWN MEP.
<i>slot/port</i>	Physical slot and port number on which MEP needs to be created.
virtual	Keyword for creating virtual MEP.
<i>agg_id</i>	Linkagg Identifier on which MEP needs to be created.
<i>vlan_id</i>	VLAN identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a maintenance endpoint.
- The *mep_id* must be unique amid all those used by or available to the service provider in the specified MA.
- The direction for virtual MEP must always be up.
- For creating a virtual MEP the value of port must be given the keyword “virtual”.

Examples

```
-> ethoam endpoint 10 domain MD association MA direction up port 1/1
-> ethoam endpoint 10 domain MD association MA direction down linkagg 1
-> ethoam endpoint 10 domain MD association MA direction down linkagg 1 vlan 10
-> ethoam endpoint 1 domain md1 association ma1 direction up port virtual primary-
vlan 100
-> no ethoam endpoint 10 domain MD association MA
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain
association end-point](#)

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
dotlagCfmMdTable
  dotlagCfmMdName
dotlagCfmMaNetTable
  dotlagCfmMaNetName
dotlagCfmMepTable
  dotlagCfmMepIdentifier
  dotlagCfmMepDirection
  dotlagCfmMepIfIndex
  dotlagCfmMepPrimaryVid
```

ethoam endpoint admin-state

Configures the administrative state of MEP.

```
ethoam endpoint mep_id domain {md_name | mac_address} association ma_name admin-state  
{enable | disable}
```

Syntax Definitions

<i>mep_id</i>	Specifies the Maintenance Association End Point. The valid range is 1–8191.
<i>md_name</i>	Specifies the domain name used while creating the management domain for which this management association is created.
<i>mac_address</i>	Specifies the CFM system MAC address.
<i>association_name</i>	Association name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
enable	Administratively enables MEP.
disable	Administratively disables MEP.

Defaults

The default value is disable.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The *mep_id* specified must already exist in the switch configuration.

Examples

```
-> ethoam endpoint 100 domain MD association MA admin-state enable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain association end-point](#) Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

DotlagCfmMep
dotlagCfmMepIndex
dotlagCfmMepIdentifier

```
dotlagCfmMepDirection  
dotlagCfmMepPortNumber  
dotlagCfmMepMacAddress  
dotlagCfmMepAdminStatus  
dotlagCfmMepFngState  
dotlagCfmMepCcmEnabled  
dotlagCfmMepCcmTransmitting  
dotlagCfmMepCcmLtmPriority  
dotlagCfmMepCcmNotReceived  
dotlagCfmMepCcmStreamError  
dotlagCfmMepCcmStreamOther  
dotlagCfmMepRdiReceived  
dotlagCfmMepLastCcmMaFault  
dotlagCfmMepLastCcmCrossConnFault  
dotlagCfmMepCcmOut  
dotlagCfmMepLbmNextSeqNumber  
dotlagCfmMepLbrIn  
dotlagCfmMepLbrInOutOfOrder  
dotlagCfmMepLbrOut  
dotlagCfmMepLtmNextSeqNumber  
dotlagCfmMepLtmIn  
dotlagCfmMepLtrOut  
dotlagCfmMepDefectsPresent  
dotlagCfmMepDefectsAbsent  
dotlagCfmMepRowStatus
```

ethoam endpoint rfp

Enables or disables the Remote Fault Propagation (RFP) on MEP.

```
ethoam endpoint mep_id domain {md_name | mac_address} association ma_name rfp {enable | disable}
```

Syntax Definitions

<i>mep_id</i>	Specifies the Maintenance Association End Point. The valid range is 1–8191.
<i>md_name</i>	Specifies the domain name used while creating the management domain for which this management association is created.
<i>mac_address</i>	Specifies the CFM system MAC address.
<i>ma_name</i>	Association name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
enable	Administratively enables RFP on MEP.
disable	Administratively disables RFP on MEP.

Defaults

The default value of RFP is disable.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The *mep_id* specified must already exist in the switch configuration.
- The domain and association must be created before RFP can be enabled.
- The MEP must be an UP MEP. If down MEP is specified, CLI returns with an error.
- The admin state of the MEP must be enabled in order to report faults.
- RFP cannot be enabled on virtual UP MEP since it is not associated with a physical interface.
- It is recommended that if RFP is enabled on a port, then any other violation feature (Link Monitoring or Link Fault Propagation) should not be configured.
- It is recommended that if RFP is enabled on a port, then automatic recovery is disabled for that port.
- If Link Monitoring is configured on a RFP enabled port, then the wait-to-restore timer must be less than the CCM interval.

Examples

```
-> ethoam endpoint 1 domain md1 association ma1 rfp enable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain association end-point](#)

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
DotlagCfmMDTable
  dotlagCfmMdName
dotlagCfmMaNetTable
  dotlagCfmMaNetName
dotlagCfmMepTable
  dotlagCfmMepIdentifier
  dotlagCfmRfpEnabled
```

ethoam endpoint ccm

Configures the MEP to generate Continuity Check Messages (CCM).

```
ethoam endpoint mep_id domain {md_name | mac_address} association ma_name  
ccm {enable | disable}
```

Syntax Definitions

<i>mep_id</i>	Specifies the Maintenance Association End Point. The valid range is 1–8191.
<i>md_name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain .
<i>mac_address</i>	Specifies the CFM system MAC address.
<i>ma_name</i>	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 10K, 6900

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain MD association MA ccm enable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain association end-point](#) Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

DotlagCfmMep

- dotlagCfmMepIndex
- dotlagCfmMepIdentifier
- dotlagCfmMepDirection
- dotlagCfmMepPortNumber
- dotlagCfmMepMacAddress
- dotlagCfmMepAdminStatus
- dotlagCfmMepFngState
- dotlagCfmMepCcmEnabled
- dotlagCfmMepCcmTransmitting
- dotlagCfmMepCcmLtmPriority
- dotlagCfmMepCcmNotReceived
- dotlagCfmMepCcmStreamError
- dotlagCfmMepCcmStreamOther
- dotlagCfmMepRdiReceived
- dotlagCfmMepLastCcmMaFault
- dotlagCfmMepLastCcmCrossConnFault
- dotlagCfmMepCcmOut
- dotlagCfmMepLbmNextSeqNumber
- dotlagCfmMepLbrIn
- dotlagCfmMepLbrInOutOfOrder
- dotlagCfmMepLbrOut
- dotlagCfmMepLtmNextSeqNumber
- dotlagCfmMepLtmIn
- dotlagCfmMepLtrOut
- dotlagCfmMepDefectsPresent
- dotlagCfmMepDefectsAbsent
- dotlagCfmMepRowStatus

ethoam endpoint priority

Configures the priority values for CCMs and Linktrace Messages (LTMs) transmitted by a MEP.

ethoam endpoint *mep_id* **domain** {*md_name* | *mac_address*} **association** *ma_name* **priority**
ccm_ltm_priority

Syntax Definitions

<i>mep_id</i>	Specifies the Maintenance Association End Point. The valid range is 1–8191.
<i>md_name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain command on page 41-5 .
<i>mac_address</i>	Specifies the CFM system MAC address.
<i>ma_name</i>	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
<i>ccm_ltm_priority</i>	Priority value for CCMs and LTMs transmitted by the MEP. The valid range is 0–7.

Defaults

parameter	default
<i>ccm_ltm_priority</i>	7

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain MD association MA priority 6
```

Release History

Release 7.3.1; command was introduced..

Related Commands

[show ethoam domain association end-point](#)

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

DotlagCfmMep

- dotlagCfmMepIndex
- dotlagCfmMepIdentifier
- dotlagCfmMepDirection
- dotlagCfmMepPortNumber
- dotlagCfmMepMacAddress
- dotlagCfmMepAdminStatus
- dotlagCfmMepFngState
- dotlagCfmMepCcmEnabled
- dotlagCfmMepCcmTransmitting
- dotlagCfmMepCcmLtmPriority
- dotlagCfmMepCcmNotReceived
- dotlagCfmMepCcmStreamError
- dotlagCfmMepCcmStreamOther
- dotlagCfmMepRdiReceived
- dotlagCfmMepLastCcmMaFault
- dotlagCfmMepLastCcmCrossConnFault
- dotlagCfmMepCcmOut
- dotlagCfmMepLbmNextSeqNumber
- dotlagCfmMepLbrIn
- dotlagCfmMepLbrInOutOfOrder
- dotlagCfmMepLbrOut
- dotlagCfmMepLtmNextSeqNumber
- dotlagCfmMepLtmIn
- dotlagCfmMepLtrOut
- dotlagCfmMepDefectsPresent
- dotlagCfmMepDefectsAbsent
- dotlagCfmMepRowStatus

ethoam endpoint lowest-priority-defect

Configures the lowest priority fault alarm for the lowest priority defect for a MEP.

ethoam endpoint *mep_id* **domain** {*md_name* | *mac_address*} **association** *ma_name* **lowest-priority-defect** *lowest_priority_defect*

Syntax Definitions

<i>mep_id</i>	Specifies the Maintenance Association End Point. The valid range is 1–8191.
<i>md_name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain command on page 41-5 .
<i>mac_address</i>	Specifies the CFM system MAC address.
<i>ma_name</i>	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
<i>lowest_priority_defect</i>	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
<i>lowest_priority_defect</i>	mac-rem-err-xcon

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The *mep_id* should be unique amid all those used by or available to the service provider in the specified MA.

Examples

```
-> ethoam endpoint 100 domain esd.alcatel-lucent.com association alcatel-sales
lowest-priority-defect all-defect
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain association end-point](#)

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

DotlagCfmMep

- dotlagCfmMepIndex
- dotlagCfmMepIdentifier
- dotlagCfmMepDirection
- dotlagCfmMepPortNumber
- dotlagCfmMepMacAddress
- dotlagCfmMepAdminStatus
- dotlagCfmMepFngState
- dotlagCfmMepCcmEnabled
- dotlagCfmMepCcmTransmitting
- dotlagCfmMepCcmLtmPriority
- dotlagCfmMepCcmNotReceived
- dotlagCfmMepCcmStreamError
- dotlagCfmMepCcmStreamOther
- dotlagCfmMepRdiReceived
- dotlagCfmMepLastCcmMaFault
- dotlagCfmMepLastCcmCrossConnFault
- dotlagCfmMepCcmOut
- dotlagCfmMepLbmNextSeqNumber
- dotlagCfmMepLbrIn
- dotlagCfmMepLbrInOutOfOrder
- dotlagCfmMepLbrOut
- dotlagCfmMepLtmNextSeqNumber
- dotlagCfmMepLtmIn
- dotlagCfmMepLtrOut
- dotlagCfmMepDefectsPresent
- dotlagCfmMepDefectsAbsent
- dotlagCfmMepRowStatus

ethoam linktrace

Enables the maintenance entity to initiate transmitting Link Trace Messages (LTM).

ethoam linktrace {**target-macaddress** *mac_address* | **target-endpoint** *t-mepid*} **source-endpoint** *s-mepid* **domain** {*d-name* | *mac_add*} **association** *a-name* [**flag** [**fdb-mpdb** | **fdbonly**]] [**hop-count** *hop_count*]

Syntax Definitions

<i>mac_add</i>	Target MAC address to be transmitted.
<i>t-mepid</i>	Specifies the MEP for which the Loopback message is targeted.
<i>s-mepid</i>	Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
<i>d-name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain .
domain <i>mac_address</i>	Specifies the CFM system MAC address.
<i>a-name</i>	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
fdbonly	Specifies that only the MAC addresses learned in a bridge's active data forwarding table will be used to decide the egress port.
<i>hop_count</i>	Indicates the number of hops remaining in this LTM. Each bridge that handles the LTM decreases the value by 1. This decreased value is returned to the LTM. The valid range is 1–2 ³² .

Defaults

parameter	default
flag	fdbonly

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command allows an operator to generate a LTM for the specified MEP.
- This command signals the MEP that it should transmit a Linktrace message and detect the presence or lack of the corresponding Linktrace messages.

Examples

```
-> ethoam linktrace target-macaddress 10:aa:ac:12:12:ad source 4 domain MD associa-
tion flag fdbonly hop-count 32
Transaction Id: 6943
```

```
-> ethoam linktrace target-endpoint 15 source 4 domain MD association
Transaction Id: 6934
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain](#)

Displays the information of a specified Management Domain configured on the bridge.

MIB Objects

DotlagCfmMep

```
dotlagCfmMepIdentifier
dotlagCfmMepTransmitLtmFlags
dotlagCfmMepTransmitLtmTargetMacAddress
dotlagCfmMepTransmitLtmTargetMepId
dotlagCfmMepTransmitLtmTargetIsmepId
dotlagCfmMepTransmitLtmTtl
dotlagCfmMepTransmitLtmResult
dotlagCfmMepTransmitEgressIdentifier
```

ethoam loopback

Initiates the transmission of loopback messages from the specified source MEP to the specified target MEP or MAC address. Also triggers the source MEP to detect the presence or lack of a corresponding loopback reply from the target.

ethoam loopback {**target-endpoint** *t-mepid* | **target-macaddress** *mac_add*} **source-endpoint** *s-mepid* **domain** *d-name* **association** *a-name* [**number** *num*] [**data** *string*] [**vlan-priority** *vlan-priority*] [**drop-eligible** { **true** | **false** }]

Syntax Definitions

<i>t-mepid</i>	Specifies the MEP for which the Loopback message is targeted. The valid range is 1-8191.
<i>mac_add</i>	Target MAC address to be transmitted.
<i>s-mepid</i>	Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
<i>d-name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain .
<i>a-name</i>	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
<i>num</i>	Number of loopback messages. Valid range is 1-10.
<i>string</i>	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.
<i>vlan-priority</i>	VLAN Priority. Valid Range is 0-7.
true	Sets the drop eligibility bit in the VLAN tag to true.
false	Sets the drop eligibility bit in the VLAN tag to false.

Defaults

parameter	default
<i>num</i>	1
<i>vlan-priority</i>	CCM priority
drop-eligible { true false }	true

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Source and target MEP-ID, MD and MA must already exist before loopback is initiated.
- If data TLV is not set, then it is not sent in the loopback message.

Examples

```
-> ethoam loopback target-endpoint 10 source-endpoint 20 domain MD association MA
number 3
Reply from 00:0E:B1:6B:43:89: bytes=64 seq=0 time=100ms
Reply form 00:0E:B1:6B:43:89: bytes=64 seq=0 time=112ms
Request timed out.
----00:E0:B1:6B:43:89 ETH-LB Statistics----
3 packets transmitted, 2 packets received, 33% packet loss
round-trip (ms)  min/avg/max = 100/106/112
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain](#)

Displays the information of a specified Management Domain configured on the bridge.

MIB Objects

```
dotlagCfmMdTable
  dotlagCfmMdName
dotlagCfmMaNetTable
  dotlagCfmMaNetName
dotlagCfmMepTable
  dotlagCfmMepIdentifier
  dotlagCfmMepTransmitLbmDestMacAddress
  dotlagCfmMepTransmitLbmDestMepId
  dotlagCfmMepTransmitLbmDestIsMepId
  dotlagCfmMepTransmitLbmMessages
  dotlagCfmMepTransmitLbmDataTlv
  dotlagCfmMepTransmitLbmVlanPriority
  dotlagCfmMepTransmitLbmVlanDropEnable
  dotlagCfmMepTransmitLbmStatus
```

ethoam fault-alarm-time

Configures the timeout value for the Fault Notification Generation Alarm time that specifies the time interval during which one or more defects should be detected before the fault alarm is issued.

ethoam fault-alarm-time *centiseconds* **endpoint** *endpoint_id* **domain** {*md_name* | *mac_address*}
association *ma_name*

no ethoam fault-alarm-time **endpoint** *endpoint_id* **domain** {*md_name* | *mac_address*}
association *ma_name*

Syntax Definitions

<i>centiseconds</i>	The Fault Notification Generation Alarm timeout value, in centiseconds. The valid range is 250–1000.
<i>endpoint_id</i>	Specifies the MEP of a specific MA. The valid range is 1–8191.
<i>md_name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain command on page 41-5 .
<i>ma_name</i>	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

Defaults

parameter	default
<i>centiseconds</i>	250

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to restore the Fault Notification Generation Alarm timeout value to the default value.
- The Fault Notification Generation Alarm timeout value is configurable per MEP.

Examples

```
-> ethoam fault-alarm-time 500 endpoint 100 domain esd.alcatel-lucent.com association alcatel_sales
-> no ethoam fault-alarm-time endpoint 100 domain esd.alcatel-lucent.com association alcatel_sales
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain
association end-point](#)

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

Dot1agCfmMep

dot1agCfmMepFngAlarmTime

ethoam fault-reset-time

Configures the timer value for the Fault Notification Generation Reset time that specifies the time interval during which the fault alarm is re-enabled to process faults. The fault alarm will only be re-enabled if no new faults are received during this time interval.

ethoam fault-reset-time *centiseconds* **endpoint** *endpoint_id* **domain** {*mac_add* | *d-name*} **association** *a-name*

no ethoam fault-reset-time endpoint *endpoint_id* **domain** {*mac_add* | *d-name*} **association** *a-name*

Syntax Definitions

<i>centiseconds</i>	The Fault Notification Generation Reset timer value, in centi seconds. The valid range is 250–1000.
<i>mep-id</i>	Specifies the MEP of a specific MA. The valid range is 1–8191.
<i>d-name</i>	Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam vlan command on page 41-3 .
<i>a-name</i>	Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

Defaults

parameter	default
<i>centiseconds</i>	1000

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to restore the Fault Notification Generation Reset timeout value to the default value.
- The Fault Notification Generation Reset timer value is configurable per MEP.

Examples

```
-> ethoam fault-reset-time 250 end-point 100 domain esd.alcatel-lucent.com associa-
tion alcatel_sales
-> no ethoam fault-reset-time end-point 100 domain esd.alcatel-lucent.com associa-
tion alcatel_sales
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[ethoam fault-alarm-time](#)

Configures the timeout value for the Fault Notification Generation Alarm time.

[show ethoam domain association end-point](#)

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

Dot1agCfmMep

dot1agCfmMepFngResetTime

ethoam one-way-delay

Initiates a one-way-delay measurement (1DM) to determine the one-way frame delay (latency) and delay variation (jitter) between two MEPs.

ethoam one-way-delay {**target-endpoint** *t-mepid* | **target-macaddress** *mac_add*} **source-endpoint** *s-mepid* **domain** *domain* **association** *association* [**vlan-priority** *vlan-priority*]

Syntax Definitions

<i>t-mepid</i>	Target MEP-ID. Valid Range 1-8191.
<i>mac_add</i>	Target MAC-Address.
<i>s-mepid</i>	Source MEP-ID. Valid Range 1-8191.
<i>domain</i>	The maintenance domain name.
<i>association</i>	The maintenance association name.
<i>vlan-priority</i>	VLAN Priority. Valid Range is 0-7.

Defaults

parameter	default
<i>vlan-priority</i>	7

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Source MEP-ID, MD and MA must be created before initiating 1DM.
- When **target-endpoint** is specified then entry must be present in the RMEP table, no matter if its status is RMEP_OK or RMEP_FAILED, before initiating 1DM. So target-macaddress can be used to bypass such a restriction.
- Although the OmniSwitch implementation of Ethernet frame delay measurement (ETH-DM) is compliant with ITU-T Y.1731, delay measurement can be performed for both ITU-T Y.1731 and IEEE 802.1ag MEPs.
- If the 1DM is initiated with a **target-macaddress** and an egress port is found for this MAC address, then the 1DM frames are transmitted from that port. Otherwise, 1DM frames are flooded in the MEP's VLAN.
- One-way delay measurement requires NTP clock synchronization between the sending and receiving MEPs.

Examples

```
-> ethoam one-way-delay target-endpoint 10 source-endpoint 12 domain MD association MA vlan-priority 4
```

```
-> ethoam one-way-dealy target-macaddress 00:e0:b1:6a:52:4c source-endpoint 12
domain MD association MA vlan-priority 4
```

Release History

Release 7.3.1; 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

```
dotlagCfmMdTable
  dotlagCfmMdName
dotlagCfmMaNetTable
  dotlagCfmMaNetName
dotlagCfmMepTable
  dotlagCfmMepIdentifier
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

<i>t-mepid</i>	Target MEP-ID. Valid Range 1-8191.
<i>mac_add</i>	Target MAC-Address.
<i>s-mepid</i>	Source MEP-ID. Valid Range 1-8191.
<i>domain</i>	The maintenance domain name.
<i>association</i>	The maintenance association name.
<i>vlan-priority</i>	VLAN Priority. Valid Range is 0-7.

Defaults

parameter	default
<i>vlan-priority</i>	7

Platforms Supported

OmniSwitch 10K, 6900

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 from 00:E0:B1:6A:52:4C: delay=2584us jitter=282us
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam two-way-delay](#) Displays the two-way-delay delay and jitter parameters for all entries or for the MAC address of a specific MEP.

MIB Objects

```
dotlagCfmMdTable
  dotlagCfmMdName
dotlagCfmMaNetTable
  dotlagCfmMaNetName
dotlagCfmMepTable
  dotlagCfmMepIdentifier
alaCfmMepTable
  alaCfmMepTWDTMacAddress
  alaCfmMepTWDTMepIdentifier
  alaCfmMepTWDTPriority
```

clear ethoam

Delete all the one-way-delay or two-way-delay entries.

```
clear ethoam {one-way-delay-table | two-way-delay-table}
```

Syntax Definitions

None

Defaults

None

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

None

Examples

```
-> clear ethoam one-way-delay-table  
-> clear ethoam two-way-delay-table
```

Release History

Release 7.3.1; 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 10K, 6900

Usage Guidelines

This command displays all the MAs for all the MDs.

Examples

```
-> show ethoam
System Configuration
  Ethernet OAM system mac address: 00:D0:95:EC:84:B0,
  Number of Maintenance Domains: 1
  Maintenance Domain: esd.alcatel-lucent.com
  Maintenance Association: alcatel-sales
```

output definitions

Ethernet OAM system mac address	The MAC address of the Ethernet OAM system.
Number of Maintenance Domains	The number of maintenance domains configured on the bridge.
Maintenance Domain	The name of the maintenance domain.
Maintenance Association	The name of the maintenance association.

Release History

Release 7.3.1; command was introduced.

Related Commands

[ethoam domain](#) Creates an Ethernet domain with a specific name.

MIB Objects

Dot1agCfmMd

dot1agCfmMdName

Dot1agCfmMa

 dot1agCfmMaName

show ethoam domain

Displays the information of a specific Management Domain configured on the bridge.

show ethoam domain *md_name*

Syntax Definitions

md_name Specifies the domain name used while creating the management domain for which this management association is created.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD
Total number of MAs configured in this MD = 1
MD Attributes
  MD-Format : string,
  MD-Level : level-3,
  MD-MHFstatus : mhfNone,
  MD-IdPermission : sendIdNone
  Maintenance Association : MA
    MA-Format : string,
    Primary Vlan : 199,
    Associated Vlan-list : none,
    Total Number of Vlans : 1,
    MA-MHFstatus : mhfNone,
    MA-IdPermission : sendIdNone,
    CCM-interval : interval10s,
    MEP-List(MEP-Id) : 10
```

output definitions

MD-level	The level at which the MD was created.
MD-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MD. Options include none , explicit , or default .
Maintenance Association	The name of the maintenance association.
Vlan	The VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 will be displayed.

output definitions (continued)

MA-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MA. Options include none , explicit , or default .
CCM-interval	The interval between the CCM transmissions.
MEP-Id	Indicates the Maintenance End Point.

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam	Displays the information of all the Management Domains (MD) configured on the bridge.
ethoam domain	Creates an Ethernet domain with a specific name.

MIB Objects

```
DotlagCfmMd
  dotlagCfmMdLevel
  dotlagCfmMdMhfCreation
DotlagCfmMa
  dotlagCfmMaName
  dotlagCfmMaVid
  dotlagCfmMaMhfCreation
  dotlagCfmMaCcmInterval
DotlagCfmMep
  dotlagCfmMepIdentifier
```

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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD association MA
Total number of MEPS configured in this MA = 1
MA-Format : string,
Primary Vlan : 100,
Associated Vlan-list : none,
Total Number of Vlans : 1,
MA-MHFstatus : mhfDefer,
MA-IdPermission : sendIdDefer,
CCM-interval : interval10s,
MEP-List(MEP-Id) : 1-5,
```

Legend: MEP-Id: * = Inactive Endpoint

MEP-ID	Admin State	Direction	Mac-Address	Port	Primary Vlan
1	disable	up	00:E0:B1:A0:78:A3	virtual	100

output definitions

Primary Vlan	The VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 will be displayed.
MA-MHFstatus	Indicates whether the maintenance entity can create MHFs for this MA. Options include none , explicit , or default .
CCM-interval	The interval between the CCM transmissions.
MEP-ID	Indicates the Maintenance End Point.

output definitions (continued)

Admin State	Indicates the administrative state (up or down) of the MEP.
Direction	The direction of the MEP.
MAC Address	The MAC address of the MEP.
Port	The slot/port number of the Bridge port to which the MEP is attached.

Release History

Release 7.3.1; command was introduced.

Related Commands

[ethoam association](#) Creates an Ethernet OAM Maintenance Association in the specified domain.

MIB Objects

DotlagCfmMa

- dotlagCfmMaVid
- dotlagCfmMaMhfCreation
- dotlagCfmMaCcmInterval

DotlagCfmMep

- dotlagCfmMepIdentifier
- dotlagCfmMepActive
- dotlagCfmMepDirection
- dotlagCfmMepIfIndex
- dotlagCfmMepMacAddress

show ethoam domain association end-point

Displays the information of a specific MEP in a Management Domain configured on the bridge.

show ethoam domain *md_name* **association** *ma_name* **end-point** *mep-id*

Syntax Definitions

<i>md_name</i>	Specifies the domain name.
<i>ma_name</i>	Name of the Ethernet OAM Association.
<i>mep-id</i>	Specifies the MEP of a specific MA. The valid range is 1–8191.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ethoam domain MD association MA endpoint 10
Admin State : disable,
Direction : up,
Slot/Port: virtual,
MacAddress: 00:E0:B1:A0:78:A3,
Fault Notification : FNG_RESET,
CCM Enabled : disabled,
RFP Status : enabled,
CCM Linktrace Priority : 7,
CCM Not Received : false,
CCM Error defect : false,
CCM Xcon defect : false,
MEP RDI defect : false,
MEP Last CCM Fault : not specified,
MEP Xcon Last CCM Fault : not specified,
MEP Error Mac Status : false,
MEP Lbm NextSeqNumber : 0,
MEP Ltm NextSeqNumber : 32157,
Fault Alarm Time : 250,
Fault Reset Time : 1000,
Lowest PrDefect Allowed : DEF_MAC_REM_ERR_XCON,
Highest PrDefect Present : DEF_NONE
```

output definitions

Admin State	Indicates the administrative state (up or down) of the MEP.
Direction	The direction of the MEP.
Slot/Port	The slot/port number of the Bridge port to which the MEP is attached.If the value is virtual, it indicates a virtual port.
MAC Address	The MAC address of the MEP.
Fault Notification	Indicates the current state of the MEP Fault Notification Generator State Machine, which can be FNG_RESET , FNG_DEFECT , FNG_REPORT_DEFECT , FNG_DEFECT_REPORTED , or FNG_DEFECT_CLEARING .
RFP Status	Indicates the status of the RFP.
CCM Enabled	Indicates whether the MEP generates CCMs (enabled) or not (disabled).
CCM Linktrace Priority	Indicates the priority value for CCMs and LTM s 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 7.3.1; command was introduced.

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

DotlagCfmMep

dotlagCfmMepActive
dotlagCfmMepDirection
dotlagCfmMepPortNumber
dotlagCfmMepMacAddress
dotlagCfmMepFngState
dotlagCfmMepCcmEnabled
dotlagCfmMepCcmLtmPriority
dotlagCfmMepSomeRMepCcmDefect
dotlagCfmMepErrorCcmDefect
dotlagCfmMepXconCcmDefect
dotlagCfmMepSomeRdiDefect
dotlagCfmMepErrorCcmLastFailure
dotlagCfmMepXconCcmLastFailure
dotlagCfmMepErrMacStatus
dotlagCfmMepLtmNextSeqNumber
dotlagCfmMepFngAlarmTime
dotlagCfmMepFngAlarmTime
dotlagCfmMepLowPrDef
dotlagCfmMepHighestPrDefect

show ethoam default-domain configuration

Displays the level, MHF, and ID permission values for the default domain.

show ethoam default-domain configuration

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ethoam default-domain configuration
Level : 3,
MHF-Creation : mhfddefault,
ID-Permission : sendIdnone
```

output definitions

Level	The level assigned to the default domain. Configured through the ethoam default-domain level command.
MHF-creation	Indicates the MHF value for a VLAN that is part of the default MD. Options include none , explicit , or default . Configured through the ethoam default-domain mhf command.
ID-Permission	The ID permission of the default domain. Configured through the ethoam default-domain id-permission command.

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam default-domain](#) Displays the primary VLAN configuration for the default domain.

MIB Objects

```
dot1agCfmMaDefaultMdDefLevel  
dot1agCfmMaDefaultMdDefMhfCreation  
dot1agCfmMaDefaultMdDefIdPermission
```

show ethoam default-domain

Displays all the default MD information for all the primary VLANs or for a specific primary VLAN.

show ethoam default-domain [**primary-vlan** *vlan_id*]

Syntax Definitions

vlan_id The primary VLAN ID.

Defaults

By default, the default MD information for all primary VLANs is displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the *vlan_id* parameter with this command to view information about the default MD for a specific primary VLAN.

Examples

```
-> show ethoam default-domain
```

Primary-Vlan	Mhf-creation	Level	Id-Permission	Status
1	mhfDefer	no-level	sendIdDefer	true
10	mhfDefault	3	sendIdNone	true

```
-> show ethoam default-domain primary-vlan 10
```

Primary-Vlan	Mhf-creation	Level	Id-Permission	Status
10	mhfDefault	3	sendIdNone	true

output definitions

Primary Vlan	The primary VLAN ID of the default MD.
Mhf-creation	The primary VLAN ID MHF value (none , explicit , or default).
Level	The primary VLAN level (no-level , 0-7).
Id-Permission	The primary VLAN ID permission (none , chassid , or defer).

Release History

Release 7.3.1; command was introduced.

Related Commands

**ethoam default-domain
primary-vlan**

Modifies the default domain for the specified primary VLAN.

MIB Objects

```
DotlagCfmDefaultMdLevel  
  dotlagCfmDefaultMdLevelVid  
  dotlagCfmDefaultMdLevelMhfCreation  
  dotlagCfmDefaultMdLevelLevel
```

show ethoam remote-endpoint domain

Displays the information of all remote MEPs learned as a part of the CCM message exchange.

show ethoam remote-endpoint domain *d_name* **association** *a_name* **end-point** *s-mepid* [**remote-mep** *r-mepid*]

Syntax Definitions

<i>d_name</i>	Specifies the domain name.
<i>a_name</i>	Specifies the name of the Ethernet OAM Association.
<i>s-mepid</i>	Specifies the MEP of a specific MA. The valid range is 1–8191.
<i>r-mepid</i>	The remote MEP. The valid range is 1–8191.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ethoam remote-endpoint domain MD association MA endpoint 10
Legends: PortStatusTlv: 1 = psBlocked, 2 = psUp, 0 = psNoTlv
          InterfaceStatusTlv: 1 = ifUp, 2 = ifDown, 4 = ifUnknown, 0=ifNoTlv
```

RMEP-ID	RMEP Status	OkFailed Time	Mac Address	port Tlv	I/f Tlv	RDI value	Ch-id Subtype	Ch-id
20	RMEP_OK	634600	00:E0:B1:6E:41:65	2	1	false	LCL-ASND	DUT-1
30	RMEP_OK	334600	00:E0:B1:6E:41:64	2	1	false	LCL-ASND	DUT-2

output definitions

MEP-ID	Indicates the Maintenance End Point.
RMEP Status	The operational state of the remote MEP Remote State machines for this MEP, which can be RMEP_IDLE , RMEP_START , RMEP_FAILED , or RMEP_OK .
OkFailed Time	The time (SysUpTime) when the Remote MEP state machine last entered either the RMEP_FAILED or RMEP_OK .
MacAddress	The MAC address of the remote MEP.

output definitions (continued)

Port Status Tlv	The MAC status TLV last received.
I/f Status Tlv	The interface status TLV last received.

Note: - Output shown above is not accurate as it is adjusted to display it in the single row. Following are modified:

P/S Tlv - Port Status Tlv
 I/F Tlv - I/F Status Tlv
 Ch-id Subtype - Chassis ID Subtype
 Ch-id - Chassis ID
 LCL-ASND - LOCALLY_ASSIGNED

Release History

Release 7.3.1; command was introduced.

Related Commands

[show ethoam domain association end-point](#) Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
dotlagCfmMepDbTable
  dotlagCfmMepDbRMepIdentifier
  dotlagCfmMepDbRMepState
  dotlagCfmMepDbRMepFailedOkTime
  dotlagCfmMepDbRdi
  dotlagCfmMepDbPortStatusTlv
  dotlagCfmMepDbInterfaceStatusTlv
  dotlagCfmMepDbChassisIdSubtype
  dotlagCfmMepDbChassisId
```

show ethoam cfmstack

Displays the contents of CFM Stack Managed Object, which determines the relationships among MEPs and MIPs on a specific bridge port.

show ethoam cfmstack {port *slot/port* | **virtual** | **linkagg** *agg_num*}

Syntax Definitions

<i>slot/port</i>	Slot and port number for which the contents of the configured MEP or MIP will be displayed.
<i>agg_num</i>	The aggregate ID for which the contents of the configured MEP or MIP will be displayed.
virtual	Virtual port.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ethoam cfmstack port 1/3
Up MHF Configured:
  Vlan-id: 100,
  Direction: up,
  MAC-Address: 00:D0:95:EC:84:B0,
  Maintenance Association: alcatel-sales,
  Maintenance Domain: esd.alcatel-lucent.com,
  MD-level: 3

Down MHF Configured:
  Vlan-id: 100,
  Direction: down,
  MAC-Address: 00:D0:95:F6:33:DA,
  Maintenance Association: alcatel-sales,
  Maintenance Domain: esd.alcatel-lucent.com,
  MD-level: 3

-> show ethoam cfmstack port virtual
MEP-Id 32 - Vlan 30:
  Direction: up,
  MAC-Address: 00:E0:B1:A5:F2:34,
  Maintenance Association: MA4,
  Maintenance Domain: MD4,
  MD-level: 4
```

output definitions

Vlan-id	The VLAN ID to which the MEP is attached.
Direction	Indicates the direction (Inward or Outward) of the Maintenance Point (MP) on the Bridge port.
MAC-Address	The MEP ID configured on this port.
Maintenance Domain	The name of the maintenance domain.
Maintenance Association	The name of the maintenance association.
MD-level	The MD level at which the MD was created.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam endpoint admin-state Creates an Ethernet OAM Maintenance End Point in the specified MA.

MIB Objects

```
DotlagCfmMd
  dotlagCfmMdName
DotlagCfmMa
  dotlagCfmMaName
DotlagCfmStack
  dotlagCfmStackVlanIdOrNone
  dotlagCfmStackDirection
  dotlagCfmStackMacAddress
  dotlagCfmStackMdLevel
```

show ethoam linktrace-reply

Displays the content of the Linktrace reply (LTR) returned by a previously transmitted LTM. This command displays the LTR based on the transaction identifier or sequence number of the LTM for which the LTR is to be displayed.

show ethoam linktrace-reply domain *d-name* **association** *a-name* **endpoint** *s-mepid* **tran-id** *num*

Syntax Definitions

<i>d-name</i>	Specifies the domain name.
<i>a-name</i>	Name of the Ethernet OAM Association.
<i>s-mepid</i>	Specifies the MEP for which LTR is to be displayed. The valid range is 1-8191.
<i>num</i>	Specifies the Transaction ID or sequence number returned from a previously transmitted LTM.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- “LTM operation successful. Target is reachable.” – This message suggests that LTM has reached the target and all the expected LTRs have been received.
- “LTM operation unsuccessful. Target not reachable.” – This message suggests that LTM is successfully initiated but the target is not reachable.
- “LTM operation unsuccessful. Target is reachable.” – This message suggest that Target is reachable but at least one of the LTR from intermediate hop is not received.
- “LTM operation in progress.” – This message suggests that LTM operation is in progress. This message will appear if show CLI is fired before LTM Time-out time.
- “LTM Timed out.”- This message suggests that either LTM is not initiated properly or when none of the expected LTRs is received in LTM Time-out duration which is 5 seconds.

Examples

```
-> show ethoam linktrace-reply domain MD association MA endpoint 10 tran-id 1256
LTM operation successful. Target is reachable.
Ttl : 63,
  LTM Forwarded : yes,
  Terminal MEP : no,
  Last Egress Identifier : 00-00:00:D0:95:EA:79:62,
  Next Egress Identifier : 00-00:00:D0:95:EA:9E:BA,
  Relay Action : RLY_FDB,
```

```

Chassis ID Subtype : LOCALLY_ASSIGNED,
Chassis ID : DUT-2,
Ingress Action : ING_OK,
Ingress Mac : 00:D0:95:EA:9E:D4,
Ingress Port ID Subtype : LOCALLY_ASSIGNED,
Ingress Port ID : 1/1,
Egress Action : EGR_OK,
Egress Mac : 00:D0:95:EA:9E:D5,
Egress Port ID Subtype : LOCALLY_ASSIGNED,
Egress Port ID : 1/2

Ttl : 62,
LTM Forwarded : no,
Terminal MEP : yes,
Last Egress Identifier : 00-00:00:D0:95:EA:9E:BA,
Next Egress Identifier : 00-00:00:00:00:00:00:00,
Relay Action : RLY_HIT,
Chassis ID Subtype : LOCALLY_ASSIGNED,
Chassis ID : DUT-3,
Ingress Action : ING_OK,
Ingress Mac : 00:D0:95:EA:AB:D2,
Ingress Port ID Subtype : LOCALLY_ASSIGNED,
Ingress Port ID : 1/1,
Egress Action : EGR_NONE,
Egress Mac : 00:00:00:00:00:00,
Egress Port ID Subtype : NONE,
Egress Port ID : none

```

output definitions

Ttl	Time to live field for the returned LTR.
LTM Forwarded	Indicates whether the LTM was forwarded or not.
Terminal MEP	Indicates whether the MP reported in the reply Ingress/Egress TLV is a MEP.
Last Egress Identifier	Identifies the MEP linktrace initiator that originated, or the responder that forwarded, the LTM to which this LTR is the response.
Next Egress Identifier	Identifies the linktrace responder that transmitted this LTR, and can forward the LTM to the next hop.
Relay Action	Indicates how the dataframe targeted by the LTM would be passed to Egress bridge port. Options include RLY_HIT , RLY_FDB , or RLY_MPDB .
Ingress Action	Indicates how the dataframe targeted by the LTM would be received on the receiving MP. Options include ING_NONE , ING_OK , ING_DOWN , ING_BLOCKED , or ING_VID .
Ingress Mac	The MAC address returned in the ingress MAC address field.
Egress Action	Indicates how the dataframe targeted by the LTM would be passed through Egress bridge port. Options include ING_NONE , ING_OK , ING_DOWN , ING_BLOCKED , or ING_VID .
Egress Mac	The MAC address returned in the egress MAC address field.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam linktrace

Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

DotlagCfmLtr

- dotlagCfmLtrTtl
- dotlagCfmLtrForwarded
- dotlagCfmLtrTerminalMep
- dotlagCfmLtrLastEgressIdentifier
- dotlagCfmLtrNextEgressIdentifier
- dotlagCfmLtrRelay
- dotlagCfmLtrIngress
- dotlagCfmLtrIngressMac
- dotlagCfmLtrEgress
- dotlagCfmLtrEgressMac

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

<i>domain_name</i>	Specifies the domain name.
<i>mac_address</i>	Specifies the CFM system MAC address.
<i>association_name</i>	Name of the Ethernet OAM Association.
<i>mep_id</i>	Specifies the MEP for which LTR is to be displayed. The valid range is 1-8191.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ethoam linktrace-tran-id domain esd.alcatel-lucent.com association alcatel-
sales endpoint 3
S.No   Transaction Id
-----+-----
      1    13357,
      2    13358,
      3    13359,
```

output definitions

S.No	Indicates the sequence number.
Transaction Id	Indicates the Transaction Identifier returned from a previously transmitted LTM.

Release History

Release 7.3.1; command was introduced.

Related Commands**ethoam linktrace**

Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

DotlagCfmLtr

dotlagCfmLtrSeqNumber

show ethoam vlan

Displays the Ethernet OAM statistics of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

show ethoam vlan *vlan-id*

Syntax Definitions

vlan-id VLAN ID, primary or non-primary VID (e.g. '10')

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.3.1; command was introduced.

Related Commands

[ethoam endpoint](#) Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

MIB Objects

```
dotlagCfmMaVlanTable
  dotlagCfmVlanVid
  dotlagCfmVlanPrimaryVid
```

show ethoam statistics

Displays the Ethernet OAM of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

show ethoam statistics domain {*domain_name* / *mac_address*} [**association** *association_name*] [**end-point** *endpoint_id*]

Syntax Definitions

<i>domain_name</i>	Specifies the domain name.
<i>mac_address</i>	Specifies the CFM system MAC address.
<i>association_name</i>	Specifies the name of Ethernet OAM Association.
<i>endpoint_id</i>	Specifies a MEP for a specific MA.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show ethoam statistics domain MD
MEP-ID  CCM   CCM Seq  LBR   LBR Out  LBR   LBR Bad  Unexpected  MA
        Out   Error    In    of order Out   MSDU    LTR In
-----+-----+-----+-----+-----+-----+-----+-----+-----
      3   105      0      0      0      0      0      0      0  MA
```

```
-> show ethoam statistics domain MD association MA
MEP-ID  CCM   CCM Seq  LBR   LBR Out  LBR   LBR Bad  Unexpected
        Out   Error    In    of order Out   MSDU    LTR In
-----+-----+-----+-----+-----+-----+-----+-----
      3   105      0      0      0      0      0      0
```

```
-> show ethoam statistics domain MD association MA endpoint 3
MEP-ID  CCM   CCM Seq  LBR   LBR Out  LBR   LBR Bad  Unexpected
        Out   Error    In    of order Out   MSDU    LTR In
-----+-----+-----+-----+-----+-----+-----+-----
      3   105      0      0      0      0      0      0
```

output definitions

MEP-Id	The MEP ID configured in the specified MA.
CCM Out	The total number of CCMs transmitted.

output definitions

CCM Seq Error	The total number of out-of-sequence CCMs received from all remote MEPs.
LBR In	The total number of valid, in-order LBRs received.
LBR Out of order	The total number of valid, out-of-order LBRs received.
LBR Out	The total number of LBRs transmitted.
LBR Bad MSDU	The total number of LBRs received whose mac_service_data_unit did not match.
Unexpected LTR In	The total number of unexpected LTRs received.

Release History

Release 7.3.1; command was introduced.

Related Commands**ethoam endpoint**

Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

MIB Objects

DotlagCfmMep

```
dotlagCfmMepIdentifier
dotlagCfmMepCcmOut
dotlagCfmMepRCcmSequenceErrors
dotlagCfmMepLbrIn
dotlagCfmMepLbrInOutOfOrder
dotlagCfmMepLbrOut
dotlagCfmMepLbrBadMsdu
dotlagCfmMepUnexpltrIn
```

show ethoam config-error

Displays the configuration error for a specified VLAN and port or linkagg.

show ethoam config-error [**vlan** *vlan_id*] [**{port** slot/port | **linkagg** *agg_id*]

Syntax Definitions

<i>vlan_id</i>	VLAN Identifier.
<i>slot/port</i>	Physical slot and port.
<i>agg_id</i>	Logical Linkagg Identifier.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
cli> show ethoam config-error
```

```
Vlan    Port    Error-type
-----+-----+-----
10      1/2     CFMleak
10      1/10    CFMleak
30      1/2     CFMleak
```

```
cli> show ethoam config-error vlan 10
```

```
vlan    port    error-type
-----+-----+-----
10      1/2     CFMleak
10      1/10    CFMleak
```

```
cli> show ethoam config-error port 1/2
```

```
vlan    port    error-type
-----+-----+-----
10      1/2     CFMleak
30      1/2     CFMleak
```

```
cli> show ethoam config-error vlan 10 port 1/2
```

```
vlan    port    error-type
-----+-----+-----
10      1/2     CFMleak
```

output definitions

vlan	VLAN identifier number.
port	Physical slot and port number.
error-type	Type of an error.

Release History

Release 7.3.1; command was introduced.

Related Commands

[ethoam linktrace](#) Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

dotlagCfmConfigErrorListTable
dotlagCfmConfigErrorListVid
dotlagCfmConfigErrorListIfIndex
dotlagCfmConfigErrorListErrorType

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

<i>domain</i>	Specifies the domain name used while creating the management domain for which this management association is created.associationPhysical slot and port.
<i>association</i>	Association name for the created Ethernet OAM Association.
<i>s-mepid</i>	Source MEP-ID. Vaild Range 1-8191.
<i>mac-add</i>	MAC-Address of the remote MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Dash ('-') in the output in Jitter column signifies that the value can not be calculated as the previous delay value is unknown. This will happen only when 1DM is received for the first time.
- Maximum entries that Delay Result table can store are 1024. After that, the oldest entry is deleted from the table whenever a new entry is required.

Examples

```
cli> show ethoam one-way-delay domain MD association MA endpoint 10
Legend: Jitter: - = undefined value
```

Remote Mac address	Delay (us)	Jitter (us)
00:d0:95:ef:44:44	2369	1258
00:d0:95:ef:66:88	5896	282
00:d0:95:ef:88:88	2584	-
00:d0:95:ef:66:55	2698	4782

```
cli> show ethoam one-way-delay domain MD association MA endpoint 10 mac-address
00:d0:95:ef:44:44
Legend: Jitter: - = undefined value
```

Remote Mac address	Delay (us)	Jitter (us)
00:d0:95:ef:44:44	2369	1258

output definitions

Remote Mac address	Remote MAC address.
Delay	Physical slot and port number.
eJitter	Type of an error.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam one-way-delay Initiates one-way-delay messages from a particular MEP to an RMEP.

MIB Objects

```

dotlagCfmMdTable
    dotlagCfmMdName
dotlagCfmMaNetTable
    dotlagCfmMaNetName
dotlagCfmMepTable
    dotlagCfmMepIdentifier
alaDotlagCfmMepDelayRsltTable
    alaDotlagCfmMepDelayRMepMacAddress
    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

<i>domain</i>	Specifies the domain name used while creating the management domain for which this management association is created.associationPhysical slot and port.
<i>association</i>	Association name for the created Ethernet OAM Association.
<i>s-mepid</i>	Source MEP-ID. Vaild Range 1-8191.
<i>mac-add</i>	MAC-Address of the remote MEP.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If '0' appears in the output in RMEP-ID column signifies that the DMM was initiated with target-macaddress. As multiple RMEPs can have same mac-address.
- If a dash ('-') appears in the output in Jitter column signifies that the value can not be calculated as the previous delay value is unknown, i.e. if only one reply for DMM (DMR) is received and this was the first time DMM was initiated from the MEP, then jitter will not be calculated.
- Maximum entries that Delay Result table can store are 1024. After that, the DMM request shall be rejected if a new entry needs to be created for the MEP. If entry for the MEP already exists in the table, that entry shall be updated with the new one.

Examples

```
cli> show ethoam two-way-delay domain MD association MA endpoint 10 mac-address
00:d0:95:ef:44:44
```

Legend: Jitter: - = undefined value

: RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address	RMEP-ID	Delay (us)	Jitter (us)
00:d0:95:ef:44:44	12	2369	1258

```
cli> show ethoam two-way-delay domain MD association MA endpoint 10 remote-mep 0
Legend: Jitter: - = undefined value
       : RMEP-ID: 0 = two-way-delay was initiated with target mac-address
```

Remote Mac address	RMEP-ID	Delay (us)	Jitter (us)
00:d0:95:ef:66:88	0	5896	282
00:d0:95:ef:88:88	0	2584	1856

```
cli> show ethoam two-way-delay domain MD association MA endpoint 10 remote-mep 15
Legend: Jitter: - = undefined value
       : RMEP-ID: 0 = two-way-delay was initiated with target mac-address
```

Remote Mac address	RMEP-ID	Delay (us)	Jitter (us)
00:d0:95:ef:66:55	15	2736	-

```
cli> show ethoam two-way-delay domain MD association MA endpoint 10
Legend: Jitter: - = undefined value
       : RMEP-ID: 0 = two-way-delay was initiated with target mac-address
```

Remote Mac address	RMEP-ID	Delay (us)	Jitter (us)
00:d0:95:ef:44:44	12	2369	1258
00:d0:95:ef:66:88	0	5896	282
00:d0:95:ef:88:88	0	2584	1856
00:d0:95:ef:66:55	15	2736	-

output definitions

Remote Mac address	Remote MAC address.
RMEP-ID	Value of RMEP-ID
Delay	Physical slot and port number.
Jitter	Type of an error.

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam two-way-delay Initiate two-way-delay messages from a particular MEP to an RMEP using target-endpoint or target-MAC address.

MIB Objects

```
dotlagCfmMdTable
  dotlagCfmMdName
dotlagCfmMaNetTable
  dotlagCfmMaNetName
dotlagCfmMepTable
  dotlagCfmMepIdentifier
```

```
alaDotlagCfmMepDelayRsltTable  
  alaCfmMepDelayRMepMacAddress  
  alaCfmMepDelayTestType  
  alaCfmMepDelayTestDelay  
  alaDotlagCfmMepDelayVariation
```

42 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
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

<i>string</i>	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”).
<i>description</i>	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”).
<i>interval</i>	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
<i>description</i>	DEFAULT
<i>interval</i>	150

Platforms Supported

OmniSwitch 10K, 6900

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 **descr** 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 **descr** 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 7.3.1; 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

<i>string</i>	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”).
<i>ipv4 addr</i>	The IPv4 address of the destination to ping.
<i>ipv4 addr</i>	The IPv4 address of the source.
<i>tos</i>	The type of service. Valid range is 0 – 255.
<i>count</i>	The number of packets to send in one ping iteration. Valid range is 1–100.
<i>delay</i>	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.
<i>size</i>	The size of the ICMP payload to be used for the ping iteration. Valid range is 24–1472 bytes.

Defaults

parameter	default
<i>count</i>	5
<i>delay</i>	1000 ms
<i>size</i>	24 bytes

Platforms Supported

OmniSwitch 10K, 6900

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 7.3.1; 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-mac mac vlan vlan-id [vlan-priority vlan-priority] [drop-eligible {true | false}] [data data] [num-pkts count] [inter-pkt-delay delay] [payload-size size] [isid-check isid]
```

Syntax Definitions

<i>string</i>	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”).
<i>mac</i>	The destination MAC address to ping.
<i>vlan-id</i>	The VLAN on which the L2 SAA Packets will be sent out. Valid range is 1-4094.
<i>vlan-priority</i>	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.
<i>data</i>	User specified string to be included in the packet.
<i>count</i>	The number of packets to send in one ping iteration. Valid range is 1–100.
<i>delay</i>	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.
<i>size</i>	The size of the ICMP payload to be used for the ping iteration. Valid range is 36–1500 bytes.
<i>isid</i>	A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network..

Defaults

parameter	default
<i>vlan-priority</i>	0
<i>drop-eligible</i>	false
<i>count</i>	5
<i>delay</i>	1000 ms
<i>size</i>	36 bytes

Platforms Supported

OmniSwitch 10K, 6900

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-mac 00:11:11:11:11:11 vlan 10
-> saa saa3 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10
drop-eligible true
->saa saa4 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10
inter-pkt-delay 100
-> saa saa5 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10
num-pkts 10
-> saa saa6 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10
payload-size 400
-> saa saa7 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10
vlan-priority 3
-> saa saa8 type mac-ping destination-mac 00:11:11:11:11:11 vlan 1001 isid-check
1002
```

Release History

Release 7.3.1; 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  
alaSaaMacCtrlIsid
```

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

<i>string</i>	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”).
<i>tmep-id</i>	The ID of the destination MEP
<i>mac</i>	The MAC address of the destination.
<i>smep-id</i>	The ID of the source MEP.
<i>domain</i>	The domain to which the source MEP belongs.
<i>assoc</i>	The association to which the source MEP belongs.
<i>priority</i>	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.
<i>data</i>	User specified string that is included in the packet.
<i>delay</i>	The delay between packets sent during a ping iteration in milliseconds. Valid range is 100 ms - 1000 ms in multiples of 100 ms.
<i>num</i>	The number of packets to be sent during loopback. Valid range is 1 - 100.

Defaults

parameter	default
drop-eligible true false	false
<i>num-pkts</i>	5
<i>delay</i>	1000

Platforms Supported

OmniSwitch 10K, 6900

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 mal vlan-priority 5 drop-eligible false
-> saa saa2 type ethoam-loopback target-endpoint 10 source endpoint 2 domain md1
association mal vlan-priority 5 drop-eligible true data « monitor association mal »
num-pkts 6 inter-pkt-delay 500
-> saa saa3 type ethoam-loopback target-endpoint 15 source endpoint 1 domain md1
association mal vlan-priority 5 drop-eligible false data « monitor association mal
» num-pkts 6
-> saa saa4 type ethoam-loopback target-endpoint 10 source endpoint 2 domain md1
association mal vlan-priority 5 drop-eligible true inter-pkt-delay 500
```

Release History

Release 7.3.1; 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

<i>string</i>	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”).
<i>tmep-id</i>	The ID of the destination MEP.
<i>mac</i>	The MAC address of the destination.
<i>smep-id</i>	The ID of the source MEP.
<i>domain</i>	The domain to which the source MEP belongs.
<i>assoc</i>	The association to which the source MEP belongs.
<i>priority</i>	The VLAN priority to be used for the outgoing packet. Valid range is 0–7.
<i>delay</i>	The delay between packets sent during a ping iteration, in milliseconds. Valid range is 100 ms - 1000 ms in multiples of 100 ms.
<i>num</i>	The number of packets to be sent during loopback. Valid range is 1–100.

Defaults

parameter	default
<i>num</i>	5
<i>delay</i>	1000

Platforms Supported

OmniSwitch 10K, 6900

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
mdl association ma1 vlan-priority 5
-> saa saa2 type ethoam-two-way-delay target-endpoint 10 source endpoint 2 domain
mdl 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
mdl association ma1 vlan-priority 5 num-pkts 6
-> saa saa4 type ethoam-two-way-delay target-endpoint 10 source endpoint 2 domain
mdl association ma1 vlan-priority 5 inter-pkt-delay 500
```

Release History

Release 7.3.1; 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

<i>string</i>	An existing SAA ID string.
<i>yyyy-mm-dd,hh:mm:ss.ds</i>	The date and time to start the SAA.

Defaults

By default, the SAA test is started immediately.

Platforms Supported

OmniSwitch 10K, 6900

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 7.3.1; 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.ds]
```

Syntax Definitions

<i>string</i>	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.
<i>yyyy-mm-dd,hh:mm:ss.ds</i>	The date and time to stop the SAA test.

Defaults

By default, the test is stopped immediately.

Platforms Supported

OmniSwitch 10K, 6900

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 saal stop  
-> saa saa2 stop never
```

Release History

Release 7.3.1; command was introduced.

Related Commands

- [show saa](#) Displays SAA configuration information.
- [show saa statistics](#) Displays SAA statistics.

MIB Objects

alaSaaCtrlTable
 alaSaaCtrlTestIndex
 alaSaaCtrlStopAt

show saa

Displays SAA configuration information.

show saa [*string* / {**descr** *description*}]

Syntax Definitions

string An existing SAA ID string.

description An existing SAA description string.

Defaults

By default, information is displayed for all configured SAAs.

Platforms Supported

OmniSwitch 10K, 6900

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 7.3.1; 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

<i>string</i>	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 10K, 6900

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    : -,
  Domain             : aricent
  Source Mep         : 4,
  Association        : ma1,
  Num-pkts           : 5,
  Inter-pkt-delay   : 500,
  Vlan-priority      : 4
SAA : saall0
  SAA-type           : ethoam-two-way-delay,
  Status             : started,
  Description        : SAA for ethernet-two-way-delay,
  Interval(minutes)  : 300,
  Destination MAC    : -,
  Destination Mep    : 5,
  Domain             : aricent
  Source Mep         : 1,
  Association        : ma2,
  Num-pkts           : 7,
  Inter-pkt-delay   : 800,
  Vlan-priority      : 5

```

Release History

Release 7.3.1; 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

<i>string</i>	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 10K, 6900

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.

Examples

```
-> show saa statistics
Legend: eth-lb = ethoam-loopback
       : eth-dmm = ethoam-two-way-delay
Legend: - = Delay or jitter value not available
Latest Record:
SAA   Type      Time of Last-Run      RTT   RTT   RTT   Jitter Jitter Jitter Pack-
ets   Description                                     Min   Avg   Max   Min   Avg   Max
Sent Rcvd
-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+
saa1 ip-ping    2009-09-05,20:18:34.0  970   1067  1432   1     99    455
7     7     DEFAULT
saa2 ip-pin     2009-09-05,20:18:48.0  1022  1180  1914   0    349    892
7     7     DEFAULT
saa3 ip-ping    2009-09-05,20:19:15.0  1016  1583  3794   8    703   2767
5     5     DEFAULT
saa4 eth-lb     2009-09-05,22:15:30.0  -     -     -     -     -     -
```

```

 8   0  DEFAULT
saa5 eth-lb 2009-09-05,22:30:40.0 1243 1537 2166 23 42 96
 6   6  DEFAULT
saa6 eth-dmm 2009-09-05,22:45:15.0 1563 2654 3574 15 27 173
 5   5  DEFAULT

```

SAA	Type	Time of Last-Run	RTT	RTT	RTT	Jitter	Jitter	Jitter
Packets	Description		Min	Avg	Max	Min	Avg	Max
Sent	Rcvd							
saal	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 : saal

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	Pack-
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	Pack-
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 saal statistics aggregate

SAA: saal

```

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 saal0 statistics

SAA: saal0

```

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 7.3.1; 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
```

43 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 to support multiple customer sites or networks distributed over the edges of a service provider network.

MIB information for the VLAN Stacking commands is as follows:

Filename: AlcatelIND1VlanStacking.MIB
Module: Alcatel-IND1-VLAN-STACKING-MIB

Filename: AlcatelIND1VlanManager.MIB
Module: Alcatel-IND1-VLAN-MGR-MIB

A summary of the available commands is listed here:

VLAN Stacking Service Mode	ethernet-service svlan ethernet-service uni-profile ethernet-service svlan source-learning ethernet-service service-name ethernet-service nni ethernet-service svlan 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 show ethernet-service vlan show ethernet-service show ethernet-service sap show ethernet-service show ethernet-service nni show ethernet-service uni show ethernet-service uni-profile show ethernet-service sap-profile
-----------------------------------	---

ethernet-service svlan

Creates a VLAN Stacking VLAN (SVLAN) for tunneling customer traffic.

```
ethernet-service svlan {svlan_id [-svlan_id2]} [admin-state {enable | disable}] [stp {enable | disable}]
[name description]
```

```
no ethernet-service svlan {svlan_id [-svlan_id2]}
```

Syntax Definitions

svlan	Creates an SVLAN for tunneling customer traffic.
<i>svlan_id</i>	The VLAN ID number identifying the SVLAN.
<i>[-svlan_id2]</i>	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.
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.
<i>description</i>	An alphanumeric string. Use quotes around the string if the VLAN name contains multiple words with spaces between them (for example, "Alcatel-Lucent Engineering").

Defaults

By default, the Spanning Tree status is enabled in both the **per-vlan** and **flat** mode when the SVLAN is created

parameter	default
enable disable	enable
stp enable disable	enable
<i>description</i>	VLAN ID number

Platforms Supported

OmniSwitch 10K, 6900

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 *svlan_id* specified already exists as a standard VLAN.

Note. Spanning Tree status for an SVLAN only applies to the Spanning Tree topology calculations for the service provider network. This status is not applied to customer VLANs (CVLANs) and does not affect the customer network topology.

Examples

```
-> ethernet-service svlan 1001-1005 admin-state enable name "Customer ABC"  
-> ethernet-service svlan 1001-1005 stp enable  
-> no ethernet-service svlan 1001
```

Release History

Release 7.1.1; command introduced.

Related Commands

[show ethernet-service vlan](#) Displays a list of SVLANs configured from the switch

MIB Objects

```
vlanTable  
  vlanNumber  
  vlanDescription  
  vlanType  
  vlanAdmStatus  
  vlanStatus
```

ethernet-service svlan source-learning

Configures the status of source learning on a VLAN Stacking VLAN (SVLAN) used for tunneling customer traffic

ethernet-service svlan *svlan1*[-*svlan2*] source-learning {enable| disable}

Syntax Definitions

svlan1 The VLAN ID number identifying the SVLAN.
[-*svlan2*] The last SVLAN ID number in a range of SVLAN IDs.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

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.
- Use the **disable** option with this command to disable the source MAC address learning.

Examples

```
-> ethernet-service svlan 20 source-learning enable  
-> ethernet-service svlan 21-25 source-learning enable  
-> ethernet-service svlan 20-25 source-learning disable
```

Release History

Release 7.1.1; command introduced.

Related Commands

[ethernet-service svlan](#) 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. A service can be carried only on a single SVLAN. All traffic within the associated service is carried on the SVLAN.

ethernet-service service-name *service-name* **svlan** *svlan_id*

no ethernet-service service-name *service-name* **svlan** *svlan_id*

Syntax Definitions

service-name

The name of the VLAN Stacking service; an alphanumeric string. Use quotes around string if the service name contains multiple words with spaces between them (for example, "Alcatel-Lucent Engineering").

svlan_id

The VLAN ID number that identifies an existing SVLAN to associate with the VLAN Stacking service.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a VLAN Stacking service. Note that when a service is removed, the SVLAN association with that service is also removed.
- If the VLAN Stacking service is associated with a Service Access Point (SAP), then remove the SAP associations before attempting to remove the VLAN Stacking service.
- Each VLAN Stacking service is associated with one SVLAN. Specifying an additional VLAN ID for an existing service is not allowed.

Examples

```
-> ethernet-service service-name Marketing svlan 10
-> no ethernet-service service-name Marketing svlan 10
```

Release History

Release 7.1.1; command introduced.

Related Commands**ethernet-service svlan**

Creates an SVLAN for customer traffic, a management VLAN for provider traffic for multicast traffic.

MIB Objects

```
alaEServiceTable  
  alaEServiceID  
  alaEServiceSVLAN  
  alaEServiceRowStatus
```

ethernet-service nni

Configures a switch port or link aggregate as a VLAN Stacking Network Network Interface (NNI) and optionally specifies the vendor TPID value and the legacy BPDU processing status for a VLAN Stacking Network Network Interface (NNI).

```
ethernet-service nni {port slot/port [-port2] | linkagg linkagg_id [-linkagg_id2]} [tpid tpid_value]
[[stp | mvrp] legacy-bpdu {enable | disable}]
```

```
no ethernet-service nni {port slot/port [-port2] | linkagg linkagg_id [-linkagg_id2]}
```

Syntax Definitions

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
[- <i>port2</i>]	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).
<i>linkagg_id</i>	The link aggregate ID.
[- <i>linkagg_id2</i>]	The last link aggregate ID number in a range of link aggregates that you want to configure.
<i>tpid_value</i>	Specifies the TPID value of the port.
enable	Enables the specified legacy BPDU support.
disable	Disables the specified legacy BPDU support.

Defaults

parameter	default
<i>tpid_value</i>	0x8100
stp legacy-bpdu enable disable	disable
mvrp legacy-bpdu enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to revert the VLAN Stacking NNI port or link aggregate back to a conventional switch port or aggregate.
- 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 cannot be configured using standard VLAN management commands.
- NNI ports can be 802.1q tagged with normal VLANs. In this case, the TPID of the packets tagged with a normal VLAN must always be 0x8100 (regardless the TPID of the NNI port). This allows NNI port to carry regular 802.1q tagged traffic as well as SVLAN tagged traffic.

- Enable legacy BPDU support only on VLAN Stacking network ports that are connected to legacy BPDU switches. Enabling legacy BPDU between AOS switches can 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 (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 MAC used:

STP

Customer MAC	{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}

- STP legacy BPDU are supported only when the **flat** Spanning Tree mode is active on the switch.

Examples

```
-> ethernet-service 10 nni port 1/3-5
-> ethernet-service 255 nni port 2/10-15 tpid 88a8
-> ethernet-service 500 nni port 1/3-5 stp legacy-bpdu enable
-> no ethernet-service 10 nni port 1/3
-> no ethernet-service 255 nni linkagg 12-15
```

Release History

Release 7.1.1; command introduced.

Related Commands

[ethernet-service svlan nni](#) Associates a switch port or link aggregate with a SVLAN.

MIB Objects

```
alaEServicePortTable
  alaEServicePortID
  alaEServicePortType
  alaEServicePortVendorTpid
  alaEServicePortLegacyStpBpdu
  alaEServicePortRowStatus
```

ethernet-service svlan nni

Associates a NNI port with a SVLAN. A network port connects to another provider bridge and carries both customer and provider traffic.

```
ethernet-service svlan {svlan_id [-svlan_id2]} nni {port slot/port[-port2] | linkagg linkagg_id [-linkagg_id2]}
```

```
no ethernet-service svlan {svlan_id [-svlan_id2]} nni {port slot/port[-port2] / linkagg linkagg_id [-linkagg_id2]}
```

Syntax Definitions

<i>svlan_id</i>	The VLAN ID number identifying the SVLAN .
<i>[-svlan_id2]</i>	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).
<i>slot/port</i>	The slot number for the module and the physical port number of a NNI port on that module (for example, 3/1 specifies port 1 on slot 3).
<i>-port2</i>	The last port number in a range of ports that you want to configure on the same slot of a NNI port (for example, 3/1-4 specifies ports 1, 2, 3, and 4 on slot 3).
<i>linkagg_id</i>	The NNI link aggregate ID number.
<i>linkagg_id2</i>	The last NNI link aggregate ID number in a range of NNI aggregates that you want to configure.

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove an association between an NNI port and an SVLAN.
- Only SVLAN IDs are accepted with this command. This SVLAN ID specified must already exist in the switch configuration.
- This command only applies to ports or link aggregates configured as VLAN Stacking NNI ports.
- NNI ports can be tagged with normal VLANs. This allows NNI ports to carry regular 802.1q tagged traffic as well as SVLAN tagged traffic.

Examples

```
-> ethernet-service svlan 10 nni port 1/3
-> ethernet-service svlan 255 nni port 2/10-15
-> ethernet-service svlan 500 nni linkagg 31-35
```



```
-> no ethernet-service svlan 10 nni port 1/3  
-> no ethernet-service svlan 255 nni port 2/12
```

Release History

Release 7.1.1; command introduced.

Related Commands

[ethernet-service svlan](#)

Creates an SVLAN for tunneling customer traffic.

[ethernet-service nni](#)

Configures a switch port or link aggregate as a VLAN Stacking NNI.

MIB Objects

```
alaEServiceNniSvlanTable  
  alaEServiceNniSvlanNni  
  alaEServiceNniSvlanSvlan  
  alaEServiceNniSvlanRowStatus
```

Related Commands

ethernet-service service-name Creates a VLAN Stacking service and associates the service with an SVLAN.

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  
  alaEServiceSapServiceID  
  alaEServiceSapProfile  
  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 {sap_id} uni {port slot/port[-port2]} / linkagg linkagg_id [-linkagg_id2]}
```

```
no ethernet-service sap {sap_id} uni {port slot/port[-port2]} / linkagg linkagg_id [-linkagg_id2]}
```

Syntax Definitions

<i>sap_id</i>	The SAP ID number identifying the service instance.
<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>-port2</i>	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).
<i>linkagg_id</i>	The link aggregate ID number.
<i>-linkagg_id2</i>	The last link aggregate ID number in a range of aggregates that you want to configure.

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 10K, 6900

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.
- Only fixed ports can be configured as UNI ports.
- The SAP ID specified with this command must already exist. Use the **ethernet-service sap** command to create a SAP.
- 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 port 1/3
-> ethernet-service sap 10 uni port 2/10-15
-> ethernet-service sap 10 uni linkagg 31-40
-> no ethernet-service sap 10 uni port 1/10-15
-> no ethernet-service sap 10 uni linkagg 31
```

Release History

Release 7.1.1; command 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 {*sap_id*} **cvlan** {**all** | *cvlan_id* | *cvlan_id1-cvlan_id2* | **untagged**}

no ethernet-service sap {*sap_id*} **cvlan** {**all** | *cvlan_id* | *cvlan_id1-cvlan_id2* | **untagged**}

Syntax Definitions

<i>sap_id</i>	The SAP ID number.
all	Applies the SAP profile to tagged and untagged frames.
<i>cvlan_id</i>	Applies the SAP profile to frames tagged with this CVLAN ID.
<i>cvlan_id1-cvlan_id2</i>	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 10K, 6900

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 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 already exist. Use the **ethernet-service sap** command to create a SAP.
- Configuring the **all** and **untagged** parameters for the same SAP is not allowed. Specify only one of these two parameters per SAP.
- Either the **all** or **untagged** parameters can be configured for the SAP. In such an instance, the default VLAN for the UNI ports associated with the SAP is changed to the VLAN assigned to the SAP related service.
- Only one SAP, with the **all** or **untagged** option, is allowed per UNI. 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** parameter or a CVLAN ID is allowed for SAP 20.

- If you do not specify **all** or **untagged** options with a UNI, then the default VLAN 4095 is set for the UNI and all untagged, untagged control traffic and unmatched tag traffic is dropped.

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
-> no ethernet-service sap 10 cvlan 200
-> no ethernet-service sap 10 cvlan all
-> no ethernet-service sap 10 cvlan 100-150
```

Release History

Release 7.1.1; command 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
  alaEServiceSapCvlanSapId
  alaEServiceSapCvlanCvlan
  alaEServiceSapCvlanMapType
  alaEServiceSapRowStatus
```

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**] [[**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*][**egress-bandwidth** *mbps*]

no ethernet-service sap-profile *sap_profile_name*

Syntax Definitions

<i>sap_profile_name</i>	An alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, "Alcatel-Lucent Engineering").
bandwidth not-assigned	Specifies that the SAP profile does not allocate switch resources to enforce bandwidth requirements. Applies only when the profile specifies the default ingress bandwidth value (zero).
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 <i>mbps</i>	The maximum amount of bandwidth to be allowed for SAP ports, for the incoming traffic, in megabits per second. This parameter can be used only along with the shared option or not-shared option.
preserve	Retains the customer VLAN ID (inner tag) and double tags the frame with the SVLAN ID (outer tag).
translate	Replaces the customer VLAN ID with the SVLAN ID.
priority not-assigned	Specifies that the SAP profile is not assigned with a priority value or priority mapping.
map-inner-to-outer-p	Maps the customer VLAN (inner tag) priority bit value to the SVLAN (outer tag) priority bit value.
map-dscp-to-outer-p	Maps the customer VLAN (inner tag) DSCP value to the SVLAN (outer tag) priority bit value.
fixed <i>value</i>	Sets the SVLAN (outer tag) priority bit to the specified value.
egress-bandwidth <i>mbps</i>	The maximum amount of bandwidth to be allowed for SAP ports, for the outgoing traffic, in megabits per second.

Defaults

parameter	default
shared not shared	shared
<i>mbps</i>	0
preserve translate	preserve
not-assigned map-inner-to-outer-p map-dscp-to-outer-p fixed <i>value</i>	fixed 0

Platforms Supported

OmniSwitch 10K, 6900

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.
- Configure the **ingress-bandwidth** or **egress-bandwidth** parameters to define rate limiting values for the SAP.

Examples

```
-> ethernet-service sap-profile video1 egress-bandwidth 10 cvlan-tag translate
priority map-inner-to-outer-p
-> ethernet-service sap-profile voice1 not-shared ingress-bandwidth 10 cvlan-tag
preserve
-> ethernet-service sap-profile voice2 shared ingress-bandwidth 10
-> no ethernet-service sap-profile video1
```

Release History

Release 7.1.1; command introduced.

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.
- show ethernet-service sap-profile** Displays the profile attribute configuration for a SAP profile.

MIB Objects

```
alaEServiceSapProfileTable  
  alaEServiceSapProfileID  
  alaEServiceSapProfileCVLANTreatment  
  alaEServiceSapProfileIngressBW  
  alaEServiceSapProfileEgressBW  
  alaEServiceSapProfilePriorityMapMode  
  alaEServiceSapProfileFixedPriority  
  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 *sap_id* **sap-profile** *sap_profile_name*

no ethernet-service sap *sap_id*

Syntax Definitions

sap_id The SAP ID number.

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 10K, 6900

Usage Guidelines

- Use the **no** form of this command along with the SAP ID to remove the SAP profile.
- If a profile association already exists for the specified SAP ID, the current profile is replaced with the profile specified with this command.
- To change the profile associated with the SAP back to the default profile, enter “default-sap-profile” with this command.
- Do not specify a service name; doing so returns 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
-> ethernet-service sap 11 sap-profile default-sap-profile
```

Release History

Release 7.1.1; command 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* [l2-protocol {**stp** | **802.1x** | **802.1ab** | **802.3ad** | **mvrp** | **amap**} {**peer** | **discard** | **tunnel**}

no ethernet-service uni-profile *uni-profile-name*

Syntax Definitions

<i>uni-profile-name</i>	Alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, "Alcatel-Lucent Engineering").
stp	Specifies how Spanning Tree BPDU is processed on the UNI port.
802.1x	Specifies how 802.1x control frames are processed on the UNI port.
802.1ab	Specifies how 802.1ab control frames are processed on the UNI port.
802.3ad	Specifies how 802.3ad and 802.3ah control frames are processed on the UNI port.
mvrp	Specifies how Multicast VLAN Registration Protocol packets are processed on the UNI port.
amap	Specifies how Alcatel Management Adjacency Protocol packets must 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.

Defaults

parameter	default
stp	tunnel
mvrp	tunnel
amap	discard
802.1x	discard
802.3ad	peer
802.1ab	discard

Platforms Supported

OmniSwitch 10K, 6900

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.
- Up to five unique UNI profile combinations, including the default profile, are allowed per switch. If a profile has the same processing settings as any other profile, then it is not considered unique.
- 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	yes	yes	yes
802.3ad	yes	yes	yes
802.1ab	yes	yes	yes
mvrp	no	yes	yes
amap	no	yes	no

- 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.
- A uni-profile cannot be modified if it is associated with a UNI. The uni-profile cannot be deleted unless the associations are deleted.

Examples

```
-> ethernet-service uni-profile uni_1 l2-protocol stp mvrp discard
-> no ethernet-service uni-profile uni_1
```

Release History

Release 7.1.1; command introduced.

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 uni	Displays the profile associations for VLAN Stacking UNI ports.
show ethernet-service uni-profile	Displays the profile attribute configuration for VLAN Stacking UNI profiles.

MIB Objects

```
alaEServiceUNIProfileTable  
  alaEServiceUNIProfileID  
  alaEServiceUNIProfileStpBpduTreatment  
  alaEServiceUNIProfile8021xTreatment  
  alaEServiceUNIProfile8021ABTreatment  
  alaEServiceUNIProfile8023adTreatment  
  alaEServiceUNIProfileMvrpTreatment  
  alaEServiceUNIProfileAmapTreatment  
  alaEServiceUNIProfileRowStatus
```

ethernet-service uni uni-profile

Associates a VLAN Stacking User Network Interface (UNI) profile with a UNI port.

```
ethernet-service uni {port slot/port[-port2] | linkagg linkagg_id [-linkagg_id2]} uni-profile  
uni-profile-name
```

```
no ethernet-service uni-profile uni-profile-name
```

Syntax Definitions

<i>slot/port</i>	The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
<i>-port2</i>	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).
<i>linkagg_id</i>	The link aggregate ID.
<i>[-linkagg_id2]</i>	The last link aggregate ID number in a range of link aggregates that you want to configure.
<i>uni_profile_name</i>	Alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, "Alcatel-Lucent Engineering").

Defaults

The default profile (default-uni-profile) is used to process control packets ingressing on a UNI port. This profile is assigned at the time a port is configured as a VLAN Stacking UNI.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command along with the **uni-profile** name to delete the uni-profile.
- This UNI specified with this command must already 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 port 1/3 uni-profile uni_1  
-> ethernet-service uni linkagg 1-5 uni-profile uni_2  
-> ethernet-service uni port 2/10-15 uni-profile default-uni-profile  
-> no ethernet-service uni-profile uni_1
```


Release History

Release 7.1.1; command 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

show ethernet-service vlan

Displays a list of SVLANs configured on the switch.

show ethernet-service vlan [*svlan_id*-[*svlan_id2*]]

Syntax Definitions

<i>svlan_id</i>	The VLAN ID number identifying the SVLAN.
- <i>svlan_id2</i>	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 are not specified with this command.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Specify a single SVLAN ID or a range of SVLAN IDs to display configuration information for the specific SVLANs.

Examples

```
-> show ethernet-service vlan
```

```

vlan          Type      name
+-----+-----+-----+
4010         svlan      Customer ABC
4020         mgmt      Provider Management
4021         svlan      Customer XYZ

```

```
-> show ethernet-service vlan 1001
```

```

Name          : VLAN 1001,
Type          : Service Vlan,
Administrative State : enabled,
Operational State  : disabled,
IP Router Port  : disabled,
IP MTU        : 1500

```

```
-> show ethernet-service vlan 1000-1004
```

```

vlan  type  admin  oper  ip    mtu  name
-----+-----+-----+-----+-----+-----+-----+
1000  vstk    Ena    Dis  Dis   1500  VLAN 1000
1001  vstk    Ena    Dis  Dis   1500  VLAN 1001
1002  vstk    Ena    Dis  Dis   1500  VLAN 1002
1003  vstk    Ena    Dis  Dis   1500  VLAN 1003
1004  vstk    Ena    Dis  Dis   1500  VLAN 1004

```

output definitions

vlan	The SVLAN ID number identifying the instance.
type	The type of SVLAN.
admin	The administrative state of the VLAN. (Ena or Dis).
oper	The operation status of the VLAN (Ena or Dis).
ip	The status of the IP router port (Ena or Dis).
mtu	The IP MTU value configured for the VLAN.
name	The user-defined text description for the SVLAN. By default, the SVLAN ID is specified for the description.

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service svlan	Creates a VLAN Stacking VLAN (SVLAN) for tunneling customer traffic, a management SVLAN for provider traffic application uses 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** *svlan_id*]

Syntax Definitions

<i>service-name</i>	The name of an existing VLAN Stacking service. Use quotes around string if the service name contains multiple words with spaces between them (for example, "Alcatel-Lucent Engineering").
<i>svlan_id</i>	The VLAN ID number that identifies an existing SVLAN .

Defaults

By default, all services are displayed if a service name or SVLAN ID is not specified with this command.

Platforms Supported

OmniSwitch 10K, 6900

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
```

```
-> 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	Displays the SVLAN ID associated with the service. Note. SVLAN appears as the field name if the VLAN ID is an 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.
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 7.1.1; command introduced.

Related Commands

- ethernet-service service-name** Creates a VLAN Stacking service and associates the service with an SVLAN .
- 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 [sap_id]
```

Syntax Definitions

sap_id The SAP ID number identifying the service instance.

Defaults

By default, all SAPs are displayed if a SAP ID is not specified with this command.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Specify a single SAP ID 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 7.1.1; command 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.
show ethernet-service sap-profile	Displays the profile attribute configuration for SAP profiles.

MIB Objects

```

alaEServiceSapTable
  alaEServiceSapID
alaEServiceSapUniTable
  alaEServiceSapUniUni
alaEServiceSapCvlanTable
  alaEServiceSapCvlanCvlan
  alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
  alaEServiceProfileID

```

show ethernet-service

Displays configuration information for a VLAN Stacking service port.

show ethernet-service port {*slot/port* / **linkagg** *linkagg_id*}

Syntax Definitions

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

linkagg_id The link aggregate ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 : 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	Displays the SVLAN ID associated with the service. Note that SVLAN appears as the field name if the VLAN ID is an 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.
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 7.1.1; command 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.
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-service nni [**port** *slot/port* / **linkagg** *linkagg_id*]

Syntax Definitions

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

linkagg_id The link aggregate ID number.

Defaults

By default, all NNI ports are displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Specify a slot/port or link aggregate ID number to display information for a single port or link aggregate ID.

Examples

```
-> show ethernet-service nni
```

```

Port          TPID          Legacy BPDU
              stp          mvrp
-----+-----+-----+-----+
1/22         0x8100        Disable      Disable
1/23         0x8100        Disable      Disable

```

```
-> show ethernet-service nni 1/23
```

```

Port          TPID          Legacy BPDU
              stp          mvrp
-----+-----+-----+-----+
1/23         0x8100        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.
stp	Whether or not Spanning Tree legacy BPDU processing is enabled for the NNI port.
mvrp	Whether or not MVRP legacy BPDU processing is enabled for the port.

Release History

Release 7.1.1; command 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.
ethernet-service nni	Configures the vendor TPID value and the legacy BPDU processing status for a VLAN Stacking Network Network Interface (NNI).
show ethernet-service	Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

```
alaEServicePortTable
  alaEServicePortID
  alaEServicePortVendorTpid
  alaEServicePortLegacyStpBpdu
  alaEServicePortLegacyGvrpBpdu
```

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 [**port** *slot/port* / **linkagg** *linkagg_id*]

Syntax Definitions

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

linkagg_id The link aggregate ID number.

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 10K, 6900

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 port 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 7.1.1; command 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-profile** Displays the profile attribute configuration for VLAN Stacking User Network Interface (UNI) profiles.

MIB Objects

```
alaEServiceUniProfileTable  
  alaEServicePortID  
  alaEServicePortProfileID
```

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 An alphanumeric string. Use quotes around the string if the profile name contains multiple words with spaces between them (for example, "Alcatel-Lucent Engineering").

Defaults

By default, all UNI profiles are displayed if a UNI profile name is not specified with this command.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Specify a UNI profile name to display attributes for a single UNI profile.

Examples

```
-> show ethernet-service uni-profile
```

```

  Profile Name      Stp      802.1x    802.3ad    802.1AB    MVRP      AMAP
+-----+-----+-----+-----+-----+-----+-----+
uprofile-video1 tunnel drop      peer      drop      tunnel    drop

```

output definitions

Profile Name	The name of the UNI profile.
Stp	Indicates how Spanning Tree traffic control packets are processed.
802.1x	Indicates how IEEE 802.1x control packets are processed.
802.3ad	Indicates how IEEE 802.3ad control packets are processed.
802.1AB	Indicates how IEEE 802.1AB control packets are processed.
MVRP	Indicates how the Multiple VLAN Registration Protocol packets are processed.
AMAP	Indicates how Alcatel-Lucent Mapping Adjacency Protocol packets are processed.

Release History

Release 7.1.1; command 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** Displays the profile associations for VLAN Stacking User Network Interface (UNI) ports.

MIB Objects

```
alaEServiceUNIProfileTable  
  alaEServiceUNIProfileID  
  alaEServiceUNIProfileStpBpduTreatment  
  alaEServiceUNIProfile8021xTreatment  
  alaEServiceUNIProfile8021ABTreatment  
  alaEServiceUNIProfile8023adTreatment  
  alaEServiceUNIProfileMvrpTreatment  
  alaEServiceUNIProfileAmapTreatment
```

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 An alphanumeric string. Use quotes around the string if the profile name contains multiple words with spaces between them (for example, "Alcatel-Lucent Engineering").

Defaults

By default, all SAP profiles are displayed if a SAP profile name is not specified with this command.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Specify a SAP profile name to display attributes for a single SAP profile.
- The ingress bandwidth value is displayed in megabytes.

Examples

```
-> show ethernet-service sap-profile
```

Profile Name	Ingr/Egr Bw	Ingr Bw Sharing	Inner Tag Option	Priority Mapping	Priority Value
default-sap-profile	0/0	Enable	Preserve	fixed	0
map_pbit	0/0	Enable	Preserve	in-out	P
sap1	24324/0	NA	Preserve	NA	NA
sap_1	0/0	NA	Preserve	NA	NA

```
-> show ethernet-service sap-profile sap-video1
```

Profile Name	Ingr/Egr Bw	Ingr Bw Sharing	Inner Tag Option	Priority Mapping	Priority Value
sap-video1	20	Disable	Preserve	NA	NA

output definitions

Profile Name	The name of the SAP profile.
Ingr/Egr Bw	Ingress Egress Bandwidth - The maximum amount of ingress and egress bandwidth to allow for SAP ports.

output definitions

Ingr Bw Sharing	Ingress Bandwidth 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.
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 (NA , in-out or fixed). 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.
Priority Value	Indicates the priority value mapped to the SVLAN (NA , default 0, a number, P , or DSCP). 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.

Release History

Release 7.1.1; command introduced.

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

```

44 Service Manager Commands

The Alcatel-Lucent OmniSwitch supports Shortest Path Bridging MAC (SPBM), as defined in the IEEE 802.1aq standard. SPBM uses the Provider Backbone Bridge (PBB) network model to encapsulate (using IEEE 802.1ah headers) and tunnel customer traffic through the network backbone. The shortest path trees (SPTs) upon which the PBB network infrastructure operates are determined using a version of the Intermediate System-to-Intermediate System (IS-IS) link state protocol that supports TLV extensions for SPB (ISIS-SPB).

The SPBM network topology consists of two layers: the backbone infrastructure (control plane) layer and the services (data plane) layer. ISIS-SPB builds the backbone layer by defining loop-free, SPTs through the backbone network. The service layer is based on the PBB framework as defined in the IEEE 802.1ah standard. SPBM supports the 802.1ah MAC-in-MAC method for data encapsulation. SPBM services transport the encapsulated traffic over the ISIS-SPB infrastructure.

The OmniSwitch Service Manager application provides the ability to configure and manage a service-based architecture consisting of the following logical entities that are required to provision a service:

- **Service Instance Identifier (I-SID).** A backbone service instance that will tunnel the encapsulated data traffic through the PBB network. The I-SID is bound to a SPB backbone VLAN (BVLAN) ID and a Service Manager SPB service ID when the service is created.
- **Access Port.** A port or link aggregate configured as an SPB access port. This type of port defines the point at which traffic from other provider networks or directly from customer networks enters the PBB network. The access port is also associated with a Layer 2 profile that specifies how to process protocol control frames received on the port
- **Service Access Point (SAP).** A SAP is a logical service entity (also referred to as a virtual port) that binds an access port to an SPB service ID and specifies the type of customer traffic ((untagged, single-tagged, double-tagged, or all) to encapsulate and tunnel through the PBB network.
- **Service Distribution Points (SDPs).** A SDP provides a logical point at which customer traffic is directed from one PE to another PE through a one-way service tunnel.

Once the SPB service-based architecture is defined, the following service components are dynamically created by the OmniSwitch. No user-configuration is required.

- **Service Distribution Point (SDP)**—A SDP provides a logical point at which customer traffic is directed from one backbone edge switch to another. SDPs are used to set up distributed services, which consist of at least one SAP on a local node, one SAP on a remote node, and an SDP binding the service on both nodes.
- **Mesh SDP**—A mesh SDP represents the binding of a SPB service instance to an SDP. The SDP then distributes the service connectivity to other backbone edge switches through the ISIS-SPB shortest path trees.

This chapter documents the Command Line Interface (CLI) commands used to configure and verify the SPB service-based architecture. For commands used to configure and verify the ISIS-SPB backbone, see [Chapter 7, “Shortest Path Bridging Commands.”](#)

MIB information for the Service Manager commands is as follows:

Filename: AlcatelIND1ServiceMgr.MIB
Module: alcatelIND1ServiceMgrMIB

A summary of the available commands is listed here:

Service Commands	service spb service spb description service spb stats service spb admin-state service spb multicast-mode service spb vlan-xlation service spb service-mtu
Service Access Port Commands	service l2profile service access service access l2profile service access vlan-xlation
Service Access Point (SAP) Commands	service spb sap service spb sap description service spb sap trusted service spb sap admin-state service spb sap stats
Clear Commands	clear service spb counters
Show Commands	show service l2profile show service access show service show service spb ports show service spb sap show service sdp show service mesh-sdp show service spb debug-info show service spb counters

service spb

Configures a Shortest Path Bridging (SPB) service and associates that service with a backbone service instance identifier (I-SID) and BVLAN. A SPB service connects multiple customer sites together across a provider-managed core network by creating a virtual zero-hop, Layer 2 switched domain.

```
service spb service_id isid instance_id bvlan bvlan_id
```

```
no service spb [service_id / all] [bvlan bvlan_id]
```

Syntax Definitions

<i>service_id</i>	A unique numerical value to identify a specific SPB service. The valid service ID range is 1–32767.
<i>instance_id</i>	A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network. The valid range is 256–16777214.
<i>bvlan_id</i>	The VLAN ID number of an existing SPB BVLAN.
all	Specifies all SPB services.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- To remove a SPB service, administratively disable the service then use the **no** form of this command and specify the service ID of the disabled service. Use the **all** parameter to remove all SPB services from the bridge configuration.
- To remove SPB services from a specific BVLAN, use the **no** form of this command with the optional **bvlan** parameter.
- SPB services created with this command are considered static services, which are identified by a service ID number between 1 and 32767 (the valid range for this command). If the SPB service was dynamically created by another OmniSwitch feature, such as Universal Network Profiles (UNP), a service ID number between 32768 and 65534 is automatically assigned to the dynamic service.
- A SPB service provides E-LAN connectivity for customer traffic and is identified by an I-SID. Services are bound to service access ports (SAPs) on the access side. On the network side they are automatically bound to service distribution points by the ISIS-SPB protocol.
- Each SPB service is basically a Virtual Forwarding Instance (VFI) that is capable of learning customer MAC addresses from the access side (SAPs) and from the network side (Mesh SDP) and then switching the traffic based on this information.

Examples

```
-> service spb 1 isid 1000 bvlan 4001
-> no service spb 1
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb description	Configures a description for the specified SPB service.
service spb stats	Configures the statistics collection status for the specified SPB service.
service spb admin-state	Configures the administrative status of the specified SPB service.
service spb multicast-mode	Configures the multicast replication mode for the specified SPB service.
service spb vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified SPB service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
  alaSvcId
  alaSvcType
  alaSvcIsid
  alaSvcBVlan
```

service spb description

Configures a description for the specified SPB service.

service spb *service_id* **description** *desc_info*

service spb *service_id* **no description**

Syntax Definitions

service_id An existing SPB service ID number.

desc_info An ASCII text string up to 160 characters in length.

Defaults

By default, a description is not added when the SPB service is created.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the description from the specified service ID.
- This command adds or modifies a description for an existing SPB service. However, the **description** parameter is also used to specify a description at the time the service is created.

Examples

Adding or modifying a description for an existing SPB service:

```
-> service spb 100 description "SPB Service for ISID 1234"  
-> service spb 10 description SPB1-CustA  
-> service spb 10 no description
```

Configuring a new service with a description:

```
-> service spb 100 isid 1234 bvlan 3000 description "SPB Service for ISID 1234"
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb	Configures a SPB service.
service spb stats	Configures the statistics collection status for the specified SPB service.
service spb admin-state	Configures the administrative status of the specified SPB service.
service spb multicast-mode	Configures the multicast replication mode for the specified SPB service.
service spb vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified SPB service.
service spb service-mtu	Configures the administrative MTU value for the specified SPB service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable  
  alaSvcId  
  alaSvcDescription
```

service spb stats

Configures ingress and egress statistics collection for packets flowing through the service access point (SAP) or service distribution point (SDP) bindings associated with the specified SPB service.

```
service spb {service_id | all} stats {enable | disable}
```

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
all	Specifies all SPB services.
enable	Administratively enables statistics gathering for the service.
disable	Administratively disables statistics gathering for the service.

Defaults

By default, statistics collection is disabled when the service is created.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command configures statistics collection for an existing SPB service. However, the **stats {enable | disable}** parameter is also used to specify the status at the time the service is created.

Examples

Configuring statistics collection for an existing SPB service:

```
-> service spb 100 stats enable
-> service spb all stats enable
-> service spb 100 stats disable
-> service spb all stats disable
```

Configuring statistics collection for a new SPB service:

```
-> service spb 200 isid 2345 bvlan 3000 stats enable
-> service spb 300 isid 3456 bvlan 2000 stats disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb	Configures a SPB service.
service spb description	Configures a description for the specified SPB service.
service spb admin-state	Configures the administrative status of the specified SPB service.
service spb multicast-mode	Configures the multicast replication mode for the specified SPB service.
service spb vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified SPB service.
service spb service-mtu	Configures the administrative MTU value for the specified SPB service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable  
  alaSvcId  
  alaSvcStatsAdminStatus
```

service spb admin-state

Configures the administrative status of the specified SPB service.

```
service spb {service_id | all} admin-state {enable | disable}
```

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
all	Specifies all SPB services.
enable	Administratively enables the service.
disable	Administratively disables the service.

Defaults

By default, the administrative status is disabled when the service is created.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Disable the administrative status of the service and any associated service access points (SAPs) and service distribution points (SDPs) before attempting to remove a SPB service.
- Disabling the administrative status does not remove the SPB service configuration from the bridge.
- This command configures the administrative status for an existing SPB service. However, the **admin-state {enable | disable}** parameter is also used to specify the status at the time the service is created.

Examples

Configuring the status for an existing SPB service:

```
-> service spb 100 admin-state enable
-> service spb all admin-state enable
-> service spb 100 admin-state disable
-> service spb all admin-state disable
```

Configuring the status for a new SPB service:

```
-> service spb 200 isid 2345 bvlan 3000 admin-state enable
-> service spb 300 isid 3456 bvlan 2000 admin-state disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb	Configures a SPB service.
service spb description	Configures a description for the specified SPB service.
service spb stats	Configures the statistics collection status for the specified SPB service.
service spb multicast-mode	Configures the multicast replication mode for the specified SPB service.
service spb vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified SPB service.
service spb service-mtu	Configures the administrative MTU value for the specified SPB service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable  
  alaSvcId  
  alaSvcAdminStatus
```

service spb multicast-mode

Configures the multicast replication mode for the specified SPB service.

```
service spb {service_id | all} multicast-mode {head-end | tandem}
```

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
all	Specifies all SPB services.
head-end	Specifies the head-in replication mode for the service.
tandem	Specifies the tandem replication mode for the service.

Defaults

By default, the service is configured to use the head-end mode.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When a SPB service is configured to use the head-in mode, a non-unicast packet received on an SPB access port is replicated once for each receiver in the provider backbone bridge (PBB) network using its unicast base MAC (BMAC) address.
- When a SPB service is configured to use the tandem mode, a non-unicast packet received on an SPB access port is replicated once at each node using the multicast group address.
- Make sure that the same multicast mode is used across all nodes for a given BVLAN. Tandem nodes and head-in nodes cannot communicate with each other.
- This command configures the multicast mode for an existing SPB service. However, the **multicast-mode {head-end | tandem}** parameter is also used to specify the status at the time the service is created.

Examples

Configuring the status for an existing SPB service:

```
-> service spb 100 multicast-mode tandem  
-> service spb 150 multicast-mode head-end
```

Configuring the status for a new SPB service:

```
-> service spb 200 isid 2345 bvlan 3000 multicast-mode tandem
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb	Configures a SPB service.
service spb description	Configures a description for the specified SPB service.
service spb stats	Configures the statistics collection status for the specified SPB service.
service spb admin-state	Configures the administrative status of the specified SPB service.
service spb vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified SPB service.
service spb service-mtu	Configures the administrative MTU value for the specified SPB service.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable  
  alaSvcId  
  alaSvcMulticastMode
```

service spb vlan-xlation

Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified SPB service.

```
service spb {service_id | all} vlan-xlation {enable | disable}
```

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
all	Specifies all SPB services.
enable	Enables VLAN translation for the service.
disable	Disables VLAN translation for the service.

Defaults

By default, VLAN translation is disabled when the service is created.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Enabling translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled.
- This command configures the VLAN translation status for an existing SPB service. However, the **vlan-xlation {enable | disable}** parameter is also used to specify the status at the time a service is created.

Examples

Configuring the status for an existing SPB service:

```
-> service spb 100 vlan-translation enable
-> service spb all vlan-translation enable
-> service spb 100 vlan-translation disable
-> service spb all vlan-translation disable
```

Configuring the status for a new SPB service:

```
-> service spb 200 isid 2345 bvlan 3000 vlan-translation enable
-> service spb 300 isid 3456 bvlan 2000 vlan-translation disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb	Configures a SPB service.
service spb description	Configures a description for the specified SPB service.
service spb stats	Configures the statistics collection status for the specified SPB service.
service spb admin-state	Configures the administrative status of the specified SPB service.
service spb multicast-mode	Configures the multicast replication mode for the specified SPB service.
service access vlan-xlation	Configures the status of VLAN Translation for the specified access port.
show service	Displays the service configuration for the bridge.

MIB Objects

```
alaSvcBaseInfoTable
  alaSvcId
  alaSvcSapVlanXlation
```

service spb service-mtu

Configures the administrative Maximum Transmission Unit (MTU) value for the specified SPB service. This value specifies the largest frame size that the service can transmit to the far-end bridge without dropping packets or requiring IP fragmentation.

service spb {*service_id* | **all**} **service-mtu** *bytes*

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
all	Specifies all SPB services.
<i>bytes</i>	The largest service frame size, in bytes, allowed through this service. The valid range is 1–9194.

Defaults

By default, the service MTU for a SPB service is set to 1514.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The service MTU and the service delineation encapsulation overhead (for example., 4 bytes for a 802.1Q tag) of the service access point (SAP) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, then the SAP is placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP is able to transition to an operative state.
- When a service is bound to a service distribution point (SDP), the service MTU is compared to the path MTU associated with the SDP. The path MTU is dynamically reduced due to the MTU capabilities discovered by the tunneling mechanism of the SDP or the egress interface MTU capabilities based on the next hop in the tunnel path.
- If the service MTU is larger than the path MTU, the SDP binding for the service is placed in an inoperative state. If the service MTU is equal to or less than the path MTU, then the SDP binding is placed in an operational state.
- This command configures the VLAN translation status for an existing SPB service. However, the **service-mtu bytes** parameter is also used to specify the status at the time a service is created.

Examples

Configuring the MTU value for an existing SPB service:

```
-> service spb 100 service-mtu 1500
-> service spb all service-mtu 1514
```

Configuring the MTU value for a new SPB service:

```
-> service spb 200 isid 2345 bvlan 3000 service-mtu 1508
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb	Configures a SPB service.
service spb description	Configures a description for the specified SPB service.
service spb stats	Configures the statistics collection status for the specified SPB service.
service spb admin-state	Configures the administrative status of the specified SPB service.
service spb multicast-mode	Configures the multicast replication mode for the specified SPB service.
service spb vlan-xlation	Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified SPB service.
show service	Displays the service configuration for the bridge.

MIB Objects

alaSvcBaseInfoTable
 alaSvcId
 alaSvcMtu

service l2profile

Configures a Layer 2 profile that is applied to an access (customer facing) port. This profile is used to specify how to process Layer 2 control frames ingressing on the access port.

service l2profile *profile-name* [**stp** | **802.1x** | **802.1ab** | **802.3ad** | **gvrp** | **mvrp** | **amap** | **pdu** | **vlan** | **uplink**] [**peer** | **discard** | **tunnel**]

no service l2profile *profile-name*

Syntax Definitions

<i>profile-name</i>	Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., "Alcatel-Lucent Engineering").
stp	Specifies how to process Spanning Tree BPDU.
802.1x	Specifies how to process 802.1x control frames.
802.1ab	Specifies how to process 802.1ab control frames.
802.3ad	Specifies how to process 802.3ad control frames.
gvrp	Specifies how to process GARP VLAN Registration Protocol packets.
mvrp	Specifies how to process Multiple VLAN Registration Protocol packets.
amap	Specifies how to process Alcatel-Lucent Management Adjacency Protocol packets.
pdu	Specifies how to process CISCO PDU.
vlan	Specifies how to process CISCO VLAN.
uplink	Specifies how to process CISCO uplinks.
peer	Allows the access port to participate in the specified protocol. Control packets are not sent to the network side of the node.
discard	Discards the specified PDU.
tunnel	Tunnels the specified PDU across the provider network.

Defaults

If no parameters are specified with this command, the new profile inherits all the following protocol settings from the default profile (**def-access-profile**):

parameter	default
stp	tunnel
802.1x	discard
802.1ab	discard
802.3ad	peer

parameter	default
gvrp	tunnel
mvrp	tunnel
amap	discard
pdu	discard
vlan	discard
uplink	discard

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to delete a Layer 2 profile. Removing the **def-access-profile** is not allowed.
- Remove any profile associations with access ports before attempting to modify or delete the profile.
- Not all of the control protocols are currently supported with the **peer**, **tunnel**, and **discard** parameters. Use the following table to determine the parameter combinations that are supported:

Protocol	Reserved MAC	peer	discard	tunnel
STP	01-80-C2-00-00-00	no	yes	yes
802.1x	01-80-C2-00-00-03	no	yes	yes
802.1ab	01-80-C2-00-00-0E	no	yes	yes
802.3ad	01-80-C2-00-00-02	yes	no	no
GVRP	01-80-C2-00-00-21	no	yes	yes
MVRP	—	no	yes	yes
AMAP	00-20-DA-00-70-04	no	yes	no
CISCO PDU	01-00-0C-CC-CC-CD	no	yes	yes
CISCO VLAN	01-00-0C-CC-CD-CE	no	yes	yes
CISCO uplink	01-00-0C-CC-CD-CF	no	yes	yes

- If a user-configured Layer 2 profile is *not* associated with an access port, then the **def-access-profile** is used to process control packets ingressing on the port.

Examples

```
-> service l2profile sap_1_profile stp discard
-> no service l2profile sap_1_profile
-> service l2profile DropL2
-> service l2profile DropL2 stp discard gvrp discard 802.1ab discard
-> service l2profile CiscoTunnel
-> service l2profile CiscoTunnel pdu tunnel vlan tunnel uplink tunnel
-> no service l2profile CiscoTunnel
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service access	Configures a switch port or link aggregate as an access port.
service access l2profile	Assigns a Layer 2 profile to the specified service access port.
show service l2profile	Displays the Layer 2 profile configuration information for the bridge.

MIB Objects

```
alaServiceMgrPortProfileTable  
  alaServiceMgrPortProfileID  
  alaServiceMgrPortProfileStpBpduTreatment  
  alaServiceMgrPortProfile8021xTreatment  
  alaServiceMgrPortProfile8021ABTreatment  
  alaEServiceUNIPProfileGvrpTreatment  
  alaServiceMgrPortProfileAmapTreatment  
  alaServiceMgrPortProfile8023ADTreatment  
  alaServiceMgrPortProfileCiscoPduTreatment  
  alaServiceMgrPortProfileCiscoVlanTreatment  
  alaServiceMgrPortProfileCiscoUplinkTreatment
```

service access

Configures a switch port or link aggregate as an access port for customer traffic.

```
service access {port slot/port[-port2] / linkagg agg_id[-agg_id2]}
```

```
no service access {port slot/port[-port2] / linkagg agg_id[-agg_id2]}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id[-agg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to revert the port mode back to the default mode (network).
- Access ports are required to configure a Service Access Point (SAP). A SAP is the point at which customer traffic enters and exits the provider service. SAPs are not configured on network ports

Examples

```
-> service access port 1/3  
-> service access linkagg 10  
-> no service access port 1/3  
-> no service access linkagg 10
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service l2profile	Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.
service access l2profile	Assigns a Layer 2 profile to the specified service access port.
show service l2profile	Displays the Layer 2 profile configuration information for the bridge.
show service access	Displays the access (customer-facing) port configuration for the bridge.

MIB Objects

```
alaServiceMgrAccessPortTable  
  alaServiceMgrPortID  
  alaServiceMgrPortMode  
  alaServiceMgrPortLinkStatus  
  alaServiceMgrPortSapType  
  alaServiceMgrSapCount
```

service access l2profile

Assigns an existing Layer 2 profile to the specified service access port. This profile determines how Layer 2 protocol frames ingressing on the access port are processed.

```
service access {port slot/port[-port2] / linkagg agg_id[-agg_id2]} l2profile {default | profile-name}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id[-agg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
default	Assigns the default profile to the specified port.
<i>profile-name</i>	The name of an existing Layer 2 profile.

Defaults

By default, the default Layer 2 profile (**def-access-profile**) is assigned when a port is configured as a service access port.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **default** parameter with this command to revert the associated profile back to the default profile settings.
- Specify only ports or link aggregates that are configured as service access ports. This command does not apply to network ports.
- Specify a profile name that already exists in the switch configuration.

Examples

```
-> service access port 1/3 l2profile sap_1_profile
-> service access linkagg 10 l2profile sap_1_profile
-> service access port 1/3 l2profile default
-> service access linkagg 10 l2profile default
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service access	Configures a switch port or link aggregate as an access port.
service l2profile	Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.
show service l2profile	Displays the Layer 2 profile configuration information for the bridge.
show service access	Displays the access (customer-facing) port configuration for the switch.

MIB Objects

```
alaServiceMgrAccessPortTable  
  alaServiceMgrPortID  
  alaServiceMgrPortMode  
  alaServiceMgrPortPortProfileID
```

service access vlan-xlation

Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified access port.

```
service access {port slot/port[-port2] / linkagg agg_id[-agg_id2]} vlan-xlation {enable | disable}
```

Syntax Definitions

<i>slot/port[-port2]</i>	The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
<i>agg_id[-agg_id2]</i>	The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
enable	Enables VLAN translation for the specified port.
disable	Disables VLAN translation for the specified port.

Defaults

By default, VLAN translation is disabled when a port or link aggregate is configured as an access port.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Specify only ports or link aggregates that are configured as service access ports. This command does not apply to SPB interfaces (network ports).
- Enabling VLAN translation on a access port implicitly enables translation for all SAPs associated with that port. However, translation must also be enabled for the services associated with these SAPs. This ensures that all SAPs associated with a service will apply VLAN translation.

Examples

```
-> service access port 1/3 vlan-xlation enable
-> service access linkagg 10 vlan-xlation enable
-> service access port 1/3 vlan-xlation disable
-> service access linkagg 10 vlan-xlation disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service access	Configures a switch port or link aggregate as an access port.
service spb vlan-xlation	Configures the status of egress VLAN translation for the specified SPB service.
show service access	Displays the access (customer-facing) port configuration for the switch.

MIB Objects

```
alaServiceMgrAccessPortTable  
  alaServiceMgrPortID  
  alaServiceMgrPortMode  
  alaServiceMgrPortVlanXlation
```

service spb sap

Configures a Service Access Point (SAP) by associating a SAP ID with a SPB service. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

```
service spb service_id sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag / :outer_qtag.inner_qtag]
```

```
service spb service_id no sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag / :outer_qtag.inner_qtag]
```

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
<i>slot/port</i>	The slot and port number of the service access port.
<i>agg_id</i>	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
<i>:qtag</i>	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
<i>:outer_qtag.inner_qtag</i>	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.

Defaults

parameter	default
:0 :all :qtag / :outer_qtag.inner_qtag	:0 (null - untagged traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove a a SAP.
- The **:all** (wildcard) parameter is also configurable as the inner tag value for double-tagged packets (for example, “10:all” specifies double-tagged packets with an outer tag equal to 10 and an inner tag with any value).
- Specify only ports or link aggregates that are configured as service access ports (see [service access](#)). This command does not apply to network ports.
- Configuring SAPs with different encapsulation types for the same access port is allowed.

Examples

```
-> service spb 100 sap port 1/1:0
-> service spb 100 sap port 1/1:50
-> service spb 100 sap port 2/10:100.200
-> service apb 100 sap port 2/10:500.all
-> service spb 100 sap linkagg 5:10
-> service spb 200 sap port 2/1:20.30
-> service spb 200 sap linkagg 9:all
-> service spb 100 no sap 2/10:100.200
-> service spb 200 no sap linkagg 9:all
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb sap description	Configures a description for the specified SAP ID.
service spb sap trusted	Configures the trust mode for the specified SAP ID.
service spb sap admin-state	Configures the administrative status for the specified SAP ID.
service spb sap stats	Configures statistics collection for the specified SAP ID.
show service spb ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
  alaSapPortId
  alaSapEncapValue
  alaSapSvcId
```

service spb sap description

Configures a description for the specified Service Access Point (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

```
service spb service_id sap {port slot/port | linkagg agg_is} [:0 | :all | :qtag | :outer_qtag.inner_qtag]
description desc_info
```

```
service spb service_id no sap {port slot/port | linkagg agg_num} [:0 | :all | :qtag |
:outer_qtag.inner_qtag] no description
```

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
<i>slot/port</i>	The slot and port number of the service access port.
<i>agg_id</i>	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
<i>:qtag</i>	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
<i>:outer_qtag.inner_qtag</i>	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
<i>desc_info</i>	An ASCII text string up to 160 characters in length.

Defaults

By default, a description is not added when the SAP is created.

parameter	default
<i>:0 :all :qtag :outer_qtag.inner_qtag</i>	:0 (null - untagged traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to remove the description from the specified SAP.
- Specify the SPB service ID number associated with the specified SAP ID (access port/encapsulation).

Examples

```
-> service spb 10 sap 1/2:10 description "CE1 to SPB10 SAP"  
-> service spb 13 linkagg 20:100.200 description "CE2 to SPB13 SAP"  
-> service spb 10 sap 1/2:10 no description  
-> service spb 13 linkagg 20:100.200 no description
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb sap	Configures a SAP by associating a SAP ID with a SPB service.
service spb sap trusted	Configures the trust mode for the specified SAP ID.
service spb sap admin-state	Configures the administrative status for the specified SAP ID.
service spb sap stats	Configures statistics collection for the specified SAP ID.
show service spb ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable  
  alaSapPortId  
  alaSapEncapValue  
  alaSapDescription  
  alaSapSvcId
```

service spb sap trusted

Configures the trust mode for the specified Service Access Port (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

A trusted SAP can accept 802.1p values in incoming packets; an untrusted SAP will set any 802.1p values to zero in incoming packets, unless an 802.1p value is configured with this command.

service spb *service_id* **sap** {**port** *slot/port* | **linkagg** *agg_num*} [**:0** | **:all** | **:qtag** | **:outer_qtag.inner_qtag**]
trusted

service spb *service_id* **sap** {**port** *slot/port* | **linkagg** *agg_num*} [**:0** | **:all** | **:qtag** | **:outer_qtag.inner_qtag**]
no trusted *priority value*

Syntax Definitions

<i>service_id</i>	An existing SPB ID number.
<i>slot/port</i>	The slot and port number of the service access port.
<i>agg_id</i>	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
:qtag	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
:outer_qtag.inner_qtag	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
trusted	Allows the SAP to use the priority value obtained from tagged packets ingressing on the SAP port. Untagged packets use the default port priority value.
<i>value</i>	The priority value to set. Values range from 0 (lowest priority) to 7 (highest priority). This is the priority assigned to tagged and untagged packets ingressing on an untrusted SAP.

Defaults

By default, the SAP is trusted with the priority set to best effort (zero). These default values are set when a port is configured as an access port and then associated with the SAP.

parameter	default
:0 :all :qtag :outer_qtag.inner_qtag	:0 (null - untagged traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no trusted** form of this command with the **priority** *value* parameter to configure a priority value to assign to packets ingressing on the SAP.
- Specify the SPB service ID number associated with the specified SAP ID (access port/encapsulation).
- Administratively disabling the SAP is not required to change the trust mode for the SAP.
- When the trust mode is changed from untrusted to trusted, the priority value is automatically set to the default best effort priority value (zero).
- Note that untagged Layer 2 control packets (for example, BPDU, GVRP, and AMAP) are always tunneled (if enabled) through the provider backbone bridge (PBB) network with the default EXP bits set to 7, so that they can arrive at the destination bridge at the highest COS queue of 7. As a result, trusted and untrusted SAPs configured on the access ports will not affect the Layer 2 control packets ingressing on the access ports.
- Configuring the trust mode on an access port is not allowed. These settings are configured for the SAP to which the access port is associated.

Examples

```
-> service spb 10 sap 1/2:10 trusted
-> service spb 13 linkagg 20 trusted
-> service spb 10 sap 1/2:10 no trusted priority 7
-> service spb 13 linkagg 20 no trusted
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb sap	Configures a SAP by associating a SAP ID with a SPB service.
service spb sap description	Configures a description for the specified SAP ID.
service spb sap admin-state	Configures the administrative status for the specified SAP ID.
service spb sap stats	Configures statistics collection for the specified SAP ID.
show service spb ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
  alaSapPortId
  alaSapEncapValue
  alaSapTrusted
  alaSapPriority
  alaSapSvcId
```

service spb sap admin-state

Configures the administrative status for the specified Service Access Point (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

```
service spb service_id sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag | :outer_qtag.inner_qtag]
admin-state {enable | disable}
```

Syntax Definitions

<i>service_id</i>	An existing SPB ID number.
<i>slot/port</i>	The slot and port number of the service access port.
<i>agg_id</i>	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
<i>:qtag</i>	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
<i>:outer_qtag.inner_qtag</i>	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
enable	Enables the administrative status of the SAP.
disable	Disables the administrative status of the SAP.

Defaults

By default, the administrative status of the SAP is disabled.

parameter	default
<i>:0</i> :all <i>:qtag</i> <i>:outer_qtag.inner_qtag</i>	:0 (null - untagged traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Specify the SPB service ID number associated with the specified SAP ID (access port/encapsulation).
- Disabling the SAP administrative status does not remove the SAP configuration from the bridge.
- If an access port goes down, all SAPs associated with that port are operationally taken down as well.

Examples

```
-> service spb 10 sap port 1/2:10 admin-state enable
-> service spb 13 linkagg 20 admin-state enable
-> service spb 10 sap port 1/2:10 admin-state disable
-> service spb 13 linkagg 20 admin-state disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[service spb sap](#)

Configures a SAP by associating a SAP ID with a SPB service.

[service spb description](#)

Configures a description for the specified SAP ID.

[service spb sap trusted](#)

Configures the trust mode for the specified SAP ID.

[service spb sap stats](#)

Configures statistics collection for the specified SAP ID.

[show service spb ports](#)

Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
  alaSapPortId
  alaSapEncapValue
  alaSapAdminStatus
  alaSapSvcId
```

service spb sap stats

Configures ingress and egress statistics collection for packets flowing through the specified SAP ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

```
service spb service_id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag | :outer_qtag.inner_qtag] stats
{enable | disable}
```

Syntax Definitions

<i>service_id</i>	An existing SPB ID number.
<i>slot/port</i>	The slot and port number of the service access port.
<i>agg_id</i>	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
<i>:qtag</i>	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
<i>:outer_qtag.inner_qtag</i>	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
enable	Enables statistics collection for the SAP.
disable	Disables statistics collection for the SAP.

Defaults

By default, statistics collection is disabled for the SAP.

parameter	default
:0 :all :qtag :outer_qtag.inner_qtag	:0 (null - untagged traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Specify the SPB service ID number associated with the specified SAP ID (access port/encapsulation).

Examples

```
-> service spb 100 sap 1/2:10 stats enable
-> service spb 101 sap linkagg 20:all stats enable
-> service spb 100 sap 1/2:10 stats disable
-> service spb 101 sap linkagg 20:all stats disable
```

Release History

Release 7.3.1; command was introduced.

Related Commands

service spb sap	Configures a SAP by associating a SAP ID with a SPB service.
service spb sap description	Configures a description for the specified SAP ID.
service spb sap trusted	Configures the trust mode for the specified SAP ID.
service spb sap admin-state	Configures the administrative status for the specified SAP ID.
show service spb ports	Displays SAP configuration information for the specified service.

MIB Objects

```
alaSapBaseInfoTable
  alaSapPortId
  alaSapEncapValue
  alaSapStatsAdminStatus
  alaSapSvcId
```

show service l2profile

Displays the Layer 2 profile configuration information for the bridge. This type of profile is applied to access (customer-facing) ports and specifies how to process Layer 2 protocol frames ingressing on such ports.

show service l2profile [*profile_name*]

Syntax Definitions

profile_name An existing Layer 2 profile name. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., "Alcatel-Lucent Engineering").

Defaults

By default, all profiles are displayed if a profile name is not specified with this command.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the *profile-name* parameter to display information for a specific profile. Entering a profile name is case sensitive.
- If there are no profiles configured for the bridge, this command still displays the information for the default profile (def-access-profile). This profile is applied to access ports that were not associated with a specific profile.

Examples

```
-> show service l2profile
Profile Name: def-access-profile,
STP      : tunnel,      802.1X   : drop,      802.3AD  : peer,      802.1AB  : drop,
GVRP     : tunnel,      AMAP    : drop,      MVRP    : tunnel      CISCO-PDU: drop,
CISCO-VLAN: drop,      CISCO-UPLINK: drop

Profile Name: DropL2,
STP      : drop,        802.1X   : drop,      802.3AD  : drop,      802.1AB  : drop,
GVRP     : drop,        AMAP    : drop,      MVRP    : tunnel      CISCO-PDU: drop,
CISCO-VLAN: drop,      CISCO-UPLINK: drop

Profile Name: CiscoTunnel,
STP      : tunnel,      802.1X   : drop,      802.3AD  : drop,      802.1AB  : drop,
GVRP     : tunnel,      AMAP    : drop,      MVRP    : tunnel      CISCO-PDU: tunnel,
CISCO-VLAN: tunnel,    CISCO-UPLINK: tunnel

->show service l2profile DropL2
Profile Name: DropL2,
STP      : drop,        802.1X   : drop,      802.3AD  : drop,      802.1AB  : drop,
GVRP     : drop,        AMAP    : drop,      MVRP    : tunnel      CISCO-PDU: drop,
CISCO-VLAN: drop,      CISCO-UPLINK: drop
```


output definitions

Profile Name	The name of the Layer 2 profile.
Stp	Indicates how Spanning Tree traffic control packets are processed.
802.1x	Indicates how IEEE 802.1x control packets are processed.
802.3ad	Indicates how IEEE 802.3ad control packets are processed.
802.1AB	Indicates how IEEE 802.1AB control packets are processed.
GVRP	Indicates how GARP VLAN Registration Protocol packets are processed.
AMAP	Indicates how Alcatel-Lucent Mapping Adjacency Protocol packets are processed.
MVRP	Indicates how Multiple VLAN Registration Protocol packets are processed.
CISCO-PDU	Indicates how CISCO PDUs are processed.
CISCO-VLAN	Indicates how CISCO VLAN PDUs are processed.
CISCO-UPLINK	Indicates how CISCO Uplink PDUS are processed.

Release History

Release 7.3.1; command was introduced.

Related Commands

service l2profile	Configures a Layer 2 profile that is applied to a service access port.
service access l2profile	Assigns an existing Layer 2 profile to the specified service access port
show service access	Displays the access (customer-facing) port configuration for the bridge.

MIB Objects

```

alaServiceMgrPortProfileTable
  alaServiceMgrPortProfileID
  alaServiceMgrPortProfileStpBpduTreatment
  alaServiceMgrPortProfileGvrpTreatment
  alaServiceMgrPortProfile8021xTreatment
  alaServiceMgrPortProfile8021ABTreatment
  alaServiceUNIPProfileGvrpTreatment
  alaServiceMgrPortProfileAmapTreatment
  alaServiceMgrPortProfile8023ADTreatment
  alaServiceMgrPortProfileMvrpTreatment
  alaServiceMgrPortProfileCiscoPduTreatment
  alaServiceMgrPortProfileCiscoVlanTreatment
  alaServiceMgrPortProfileCiscoUplinkTreatment

```

show service access

Displays the access (customer-facing) port configuration for the bridge.

show service access [**port** *slot/port* / **linkagg** *agg_id*]

Syntax Definitions

slot/port

The slot and port number of the service access port.

agg_id

The link aggregate ID number (0–31) of a service access link aggregate.

Defaults

By default, all service access ports are displayed if a port or link aggregate number is not specified.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use the **port** *slot/port* and **linkagg** *agg-id* parameters to display the configuration for a specific port or link aggregate.

Examples

```
-> show service access
```

Port Id	Link Status	SAP Type	SAP Count	Vlan Xlation	L2Profile
1/11	Up	Manual	100	N	def-access-profile
1/12	Up	Manual	100	N	def-access-profile
1/13	Down	Manual	100	N	def-access-profile
1/14	Down	Manual	100	N	def-access-profile

Total Access Ports: 4

```
-> show service access port 1/14
```

Port Id	Link Status	SAP Type	SAP Count	Vlan Xlation	L2Profile
1/14	Down	Manual	100	N	def-access-profile

Total Access Ports: 4

output definitions

Port Id	The access port number or link aggregate ID number.
Link Status	The status of the link connection to the access port (Up or Down).
SAP Type	Whether or not the SAP associate with the access port was created statically or dynamically (Manual or Dynamic).
SAP Count	The number of service access points (SAPs) that are associated with the access port.

output definitions

VLAN Xlation	Whether or not VLAN translation is enabled on the access port.
L2Profile	The name of the Layer 2 profile associated with the access port. Configured through the service l2profile command.

Release History

Release 7.3.1; command was introduced.

Related Commands

service access	Configures a switch port or link aggregate as a service access port.
show service l2profile	Displays the Layer 2 profile configuration for the bridge.

MIB Objects

```
alaServiceMgrPortTable
  alaServiceMgrPortID
  alaServiceMgrPortLinkStatus
  alaServiceMgrPortSapType
  alaServiceMgrPortSapCount
  alaServiceMgrPortVlanXlation
  alaServiceMgrPortPortProfileID
```

show service

Displays the service configuration for the bridge.

show service [spb]

Syntax Definitions

spb Displays Shortest Path Bridging (SPB) services.

Defaults

By default, all services are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **spb** parameter to display additional information about SPB services.
- The service ID is a unique number that identifies a specific SPB service. Information associated with the service ID is displayed.

Examples

```
-> show service
Legend: * denotes a dynamic object
All Service Info
```

ServiceId	Svc Type	Adm	Opr	Stats	SAP Count	Bind Count	Description
100	SPB	Up	Down	Y	8	4	SPB Service 100
200	SPB	Up	Up	Y	7	5	SPB Service 200
32768*	SPB	Up	Up	Y	23	4	SPB Dynamic Service 32768
32769*	SPB	Up	Up	Y	10	3	SPB Dynamic Service 32769

Total Services: 4

```
-> show service spb
Legend: * denotes a dynamic object
SPB Service Info
  SystemId : 00e0.ble7.0188,   SrcId : 0x70188,   SystemName : TOR-1
```

ServiceId	Adm	Oper	Stats	SAP Count	Bind Count	Isid	BVlan	MCast Mode	(T/R)
100	Up	Down	Y	8	4	1000	4001	Headend	(0/0)
200	Up	Up	Y	7	5	1001	4001	Headend	(0/0)
32768*	Up	Up	Y	23	4	1002	4001	Headend	(0/0)
32769*	Up	Up	Y	10	3	1003	4001	Headend	(0/0)

output definitions

ServiceId	The service ID number.
Svc Type	The type of service (only SPB is supported).
Adm	The administrative state of the service (Up or Down).
Opr	The operational state of the service (Up or Down).
Stats	Whether or not statistics collection is enabled for the service.
SAP Count	The number of service access points (SDPs) associated with this SPB service.
Bind Count	The number of service distribution points (SDPs) bound to this SPB service.
Description	An optional description configured for the service.
ISID	The service instance identifier that identifies the SPB service instance within the provider backbone bridging (PBB) network.
BVLAN	The VLAN ID number for the base VLAN to which the SPB service is mapped.
Mcast Mode	The multicast replication mode (Headend or Tandem) for the service.

Release History

Release 7.3.1; command was introduced.

Related Commands

show service sdp	Displays the SDP configuration for the bridge.
show service mesh-sdp	Displays the Mesh SDP bindings for the bridge.

MIB Objects

```

alaSvcBaseInfoTable
  alaSvcId
  alaSvcType
  alaSvcAdminStatus
  alaSvcOperStatus
  alaSvcStatsAdminStatus
  alaSvcNumSaps
  alaSvcNumSdps
  alaSvcDescription
  alaSvcIsid
  alaSvcBVlan
  alaSvcMulticastMode

```

show service spb ports

Displays the virtual ports associated with the specified SPB service.

show service spb *service_id* ports

Syntax Definitions

service_id An existing SPB service ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is associated with the specified SPB service.
- In addition to the virtual port configuration, this command also provides the status and additional configuration information for the SPB service.

Examples

```
-> show service spb 1525 ports
```

Legend: * denotes a dynamic object

SPB Service Info

```
Admin : Up, Oper : Up, Stats : N, Mtu : 1514, VlanXlation : N,
ISID : 2524, BVlan : 4004, MCast-Mode : Headend, Tx/Rx : 0/0
```

Identifier	Adm	Oper	Stats	Sap Trusted:Priority/ Sdp SystemId:BVlan	Intf	Sap Description / Sdp SystemName
sap:1/11:2524	Up	Up	N	Y:x	1/11	-
sap:1/12:2524	Up	Up	N	Y:x	1/12	-
sap:1/13:2524	Up	Down	N	Y:x	1/13	-
sap:1/14:2524	Up	Down	N	Y:x	1/14	-
sdp:32806:1525*	Up	Up	Y	e8e7.3233.1831:4004	1/1	BRIDGE-4

Total Ports: 5

output definitions

Identifier	The virtual ports (SAPs or SDPs) associated with the service.
Adm	The administrative state of the virtual port (Up or Down).
Oper	The operational state of the virtual port (Up or Down).
Stats	Whether or not statistics collection is enabled for the virtual port.
Sap Trusted : Priority	Whether or not the Service Access Point (SAP) virtual port associated with the service is trusted or assigns a priority value.

output definitions

Sdp SystemId : BVlan	The system ID (base MAC) and associated BVLAN for a Service Distribution Point (SDP) virtual port associated with the service.
Intf	The bridge interface (port or link aggregate) of the virtual port (SAP or SDP) that is associated with the service.
Sap Description	The description for the SAP that is associated with the service.
Sdp Systemname	The system name for the SDP bridge that is associated with the service.

Release History

Release 7.3.1; command was introduced.

Related Commands

[show service](#)

Displays the service configuration for the bridge.

[show service spb sap](#)

Displays the service access point (SAP) configuration for a specific SAP associated with the specified SPB service.

MIB Objects

N/A

show service spb sap

Displays the configuration information for the specified SAP ID associated with the specified service. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

show service spb *service_id* **sap** {*slot/port* | **linkagg** *agg_num*} [**:0** | **:all** | *:qtag* | **:outer_qtag.inner_qtag**]

Syntax Definitions

<i>service_id</i>	An existing SPB ID number.
<i>slot/port</i>	The slot and port number of the service access port.
<i>agg_id</i>	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
<i>:qtag</i>	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
<i>:outer_qtag.inner_qtag</i>	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A Service Access Point (SAP) is a type of virtual port that is associated with the specified SPB service.
- A SAP determines which customer traffic (untagged, single-tagged, or double-tagged) is mapped to the service associated with this SAP.

Examples

```
-> show service spb 1525 sap port 1/11:2524
SAP Detailed Info
  SAP Id           : 1/11:2524,           Description      : ,
  Admin Status     : Up,                 Oper Status     : Up,
  Stats Status     : No,                 Vlan Translation : No,
  Service Type     : SPB,                 Allocation Type  : Static,
  Trusted          : Yes,                 Priority        : 0,
  Ingress Pkts    : 0,                   Ingress Bytes   : 0,
  Egress Pkts     : 0,                   Egress Bytes    : 0,
```


Mgmt Change : 08/08/2012 05:41:39, Status Change : 08/10/2012 21:14:42

output definitions

SAP Id	The access port and encapsulation associated with the service.
Description	An optional description configured for the SAP. By default, the description is blank.
Admin Status	The administrative state of the SAP (Up or Down).
Oper Status	The operational state of the SAP (Up or Down).
Stats Status	Whether or not statistics collection is enabled for the SAP (Yes or No).
Vlan Translation	Whether or not VLAN translation is enabled for the SAP (Yes or No).
Service Type	The type of service associated with this SAP (only SPB supported).
Allocation Type	Whether the service was manually or dynamically created (Static or Dynamic).
Trusted	Whether or not the SAP is trusted (Yes or No).
Priority	The 802.1p priority assigned to traffic mapped to this SAP. Applied only when SAP is not trusted and a priority is specified.
Ingress Pkts	The number of packets that have ingress on this SAP.
Ingress Bytes	The number of bytes that have ingress on this SAP.
Egress Pkts	The number of packets that have egress on this SAP.
Egress Bytes	The number of bytes that have egress on this SAP.
Mgmt Change	The date and time of the last configuration change for this SAP.
Status Change	The date and time of the last operational status change for this SAP.

Release History

Release 7.3.1; command was introduced.

Related Commands

show service	Displays the service configuration for the bridge.
show service spb ports	Displays the virtual ports (SAP and SDPs) associated with the specified SPB service.

MIB Objects

N/A

show service sdp

Displays the Service Distribution Point (SDP) configuration for the bridge. A SDP is a logical entity that directs traffic from one Backbone Edge Bridge (BEB) to another BEB in the Provider Backbone Bridge (PBB) network.

show service sdp [spb]

Syntax Definitions

spb Displays Shortest Path Bridging (SPB) SDPs.

Defaults

By default, all SDPs are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **spb** parameter to display additional information about SPB SDPs.
- There is no manual configuration of SDPs required. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the PBB network.
- Dynamic SDPs are not saved to the switch configuration file.

Examples

```
-> show service sdp
```

Legend: * denotes a dynamic object

All SDP Info

SdpId	FarEnd SysId:BVlan	Adm	Oper	SvcType
32817*	00e0.b1e7.0bd3:4001	Up	Up	SPB
32818*	e8e7.3200.2a1d:4001	Up	Up	SPB
32821*	e8e7.3200.2a1d:4002	Up	Up	SPB
32823*	00e0.b1e7.0bd3:4003	Up	Up	SPB
32824*	e8e7.3200.2a1d:4003	Up	Up	SPB
32827*	e8e7.3200.2a1d:4004	Up	Up	SPB
32832*	e8e7.3233.1c81:4001	Up	Up	SPB
32834*	00e0.b1e7.0bd3:4002	Up	Up	SPB
32835*	e8e7.3233.1c81:4002	Up	Up	SPB

output definitions

SdpId	The unique SDP identification number that is dynamically generated by ISIS-SPB.
FarEnd SysId:BVlan	The System ID (bridge MAC address) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.
Adm	The administrative state of the SDP (Up or Down).

output definitions

Opr	The operational state of the SDP (Up or Down).
Svc Type	The type of service bound to the SDP (only SPB is supported).

-> show service sdp spb

Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB SDP Info

SdpId	FarEnd SysId:BVlan/GroupMac	SourceId	Oper	Intf/Isid	Bind Count	FarEnd SystemName/PortList
32817*	00e0.b1e7.0bd3:4001	0x70bd3	Up	1/3	0	BRIDGE-2
32818*	e8e7.3200.2a1d:4001	0x2a1d	Up	1/3	0	BRIDGE-3
32821*	e8e7.3200.2a1d:4002	0x2a1d	Up	1/3	0	BRIDGE-3
32823*	00e0.b1e7.0bd3:4003	0x70bd3	Up	1/3	0	BRIDGE-2
32824*	e8e7.3200.2a1d:4003	0x2a1d	Up	1/3	0	BRIDGE-3
32827*	e8e7.3200.2a1d:4004	0x2a1d	Up	1/3	0	BRIDGE-3
32832*	e8e7.3233.1c81:4001	0x31c81	Up	1/2	0	BRIDGE-8
32834*	00e0.b1e7.0bd3:4002	0x70bd3	Up	1/2	0	BRIDGE-2
32835*	e8e7.3233.1c81:4002	0x31c81	Up	1/2	0	BRIDGE-8

output definitions

SdpId	The unique SDP identification number that is dynamically generated by ISIS-SPB.
FarEnd SysId:BVlan/ GroupMac	The System ID (BMAC) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.
SourceId	The shortest path (SP) source ID of the bridge.
Opr	The operational state of the SDP (Up or Down).
Intf/Isid	The SPB interface (network port) on which ISIS-SPB discovered the neighbor BMAC and BVLAN.
Bind Count	The number of services bound to this SDP.
FarEnd SystemName / PortList	The system name and port list of the far-end SPB node.

Release History

Release 7.3.1; command was introduced.

Related Commands

show service	Displays the service configuration for the bridge.
show service mesh-sdp	Displays the Mesh SDP configuration for the bridge.

MIB Objects

```
alaSdpBaseInfoTable  
  alaSdpId  
  alaSdpAdminStatus  
  alaSdpOperStatus  
  alaSdpNetworkPort  
  alaSvcBVlan  
  alaSdpSystemId  
  alaSdpSystemName  
  alaSdpSpSourceId
```

show service mesh-sdp

Displays the mesh Service Distribution Point (SDP) binding configuration for the bridge. Once a SDP is established and ISIS-SPB detects a service on the far-end SPB node that also exists on the local node, the SDP (BMAC:BVLAN) is automatically bound to the service instance.

show service mesh-sdp [spb]

Syntax Definitions

spb Displays Shortest Path Bridging (SPB) mesh SDPs.

Defaults

By default, all mesh SDPs are displayed.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **spb** parameter to display additional information about SPB mesh SDPs.
- There is no manual configuration of mesh SDPs required. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the provider backbone bridge (PBB) network.
- Dynamic mesh SDPs are not saved to the switch configuration file.

Examples

```
-> show service mesh-sdp
```

Legend: * denotes a dynamic object

All Mesh-SDP Info

SvcId	SdpId	FarEnd SysId:Bvlan	Oper	SvcType
1	33687:1*	e8e7.3233.1831:4001	Up	SPB
1	37753:1*	0000.bcb6.0001:4001	Up	SPB
1	38169:1*	0000.bcb4.0001:4001	Up	SPB
1	38217:1*	0000.beb4.0001:4001	Up	SPB
1	38218:1*	0000.beb4.0002:4001	Up	SPB
1	38219:1*	0000.beb4.0003:4001	Up	SPB
1	38220:1*	0000.beb4.0004:4001	Up	SPB
1	38221:1*	0000.beb4.0005:4001	Up	SPB
1	38222:1*	0000.beb4.0006:4001	Up	SPB
1	38223:1*	0000.beb4.0007:4001	Up	SPB

output definitions

ServiceId	The ID number of the service that is bound to the SDP.
SdpId	The unique SDP identification number that is dynamically generated by ISIS-SPB and bound to the service number.
FarEnd SysId:Bvlan	The System ID (bridge MAC address) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.

output definitions

Opr	The operational state of the SDP (Up or Down).
Svc Type	The type of service bound to the SDP (only SPB is supported).

-> show service mesh-sdp spb

Legend: * denotes a dynamic object

SPB Mesh-SDP Info

SvcId	SdpId	Isid	FarEnd SysId:BVlan	Oper	Intf	FarEnd SystemName
1	33687:1*	1000	e8e7.3233.1831:4001	Up	1/1	Bridge-4
1	37753:1*	1000	0000.bcb6.0001:4001	Up	1/1	Ix-SPB-6
1	38169:1*	1000	0000.bcb4.0001:4001	Up	1/1	Ix-SPB-4
1	38217:1*	1000	0000.beb4.0001:4001	Up	1/1	Ix-BEB-4.1.1
1	38218:1*	1000	0000.beb4.0002:4001	Up	1/1	Ix-BEB-4.1.2
1	38219:1*	1000	0000.beb4.0003:4001	Up	1/1	Ix-BEB-4.1.3
1	38220:1*	1000	0000.beb4.0004:4001	Up	1/1	Ix-BEB-4.2.1
1	38221:1*	1000	0000.beb4.0005:4001	Up	1/1	Ix-BEB-4.2.2
1	38222:1*	1000	0000.beb4.0006:4001	Up	1/1	Ix-BEB-4.2.3
1	38223:1*	1000	0000.beb4.0007:4001	Up	1/1	Ix-BEB-4.3.1

output definitions

ServiceId	The ID number of the service that is bound to the SDP.
SdpId	The unique SDP identification number that is dynamically generated by ISIS-SPB and bound to the service number.
FarEnd SysId:BVlan/ GroupMac	The System ID (BMAC) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.
Opr	The operational state of the mesh SDP (Up or Down).
Intf	The SPB interface (network port) on which ISIS-SPB discovered the neighbor BMAC and BVLAN.
FarEnd SystemName	The system name of the far-end SPB node.

Release History

Release 7.3.1; command was introduced.

Related Commands

show service	Displays the service configuration for the bridge.
show service sdp	Displays the SDP configuration for the bridge.

MIB Objects

```

alaSdpBindTable
  alaSdpBindId
  alaSdpBindOperStatus
  alaSdpBindNetworkPort
  alaSdpBindVirtualPort
  alaSdpBindIsid
  alaSdpBindBVlan
  alaSdpBindSystemId
  alaSdpBindSystemName

```

show service spb debug-info

Displays debug information for the virtual ports associated with the SPB service.

show service spb *service_id* **ports**

Syntax Definitions

service_id An existing SPB service ID number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is associated with the specified SPB service.
- In addition to the virtual port configuration, this command also provides the status and additional configuration information for the SPB service.

Examples

```
-> show service spb 1525 ports
```

Legend: * denotes a dynamic object

SPB Service Info

```
Admin : Up, Oper : Up, Stats : N, Mtu : 1514, VlanXlation : N,
ISID : 2524, BVlan : 4004, MCast-Mode : Headend, Tx/Rx : 0/0
```

Identifier	Adm	Oper	Stats	Sap Trusted:Priority/ Sdp SystemId:BVlan	Intf	Sap Description / Sdp SystemName	UP
sap:1/11:2524	Up	Up	N	Y:x	1/11	-	100
sap:1/12:2524	Up	Up	N	Y:x	1/12	-	200
sap:1/13:2524	Up	Down	N	Y:x	1/13	-	300
sap:1/14:2524	Up	Down	N	Y:x	1/14	-	400
sdp:32806:1525*	Up	Up	Y	e8e7.3233.1831:4004	1/1	TOR-4	404

Total Ports: 5

output definitions

Identifier	The virtual ports (SAPs or SDPs) associated with the service.
Adm	The administrative state of the virtual port (Up or Down).
Oper	The operational state of the virtual port (Up or Down).
Stats	Whether or not statistics collection is enabled for the virtual port.
Sap Trusted : Priority	Whether or not the Service Access Point (SAP) virtual port associated with the service is trusted or assigns a priority value.

output definitions

Sdp SystemId : BVlan	The system ID (base MAC) and associated BVLAN for a Service Distribution Point (SDP) virtual port associated with the service.
Intf	The bridge interface (port or link aggregate) of the virtual port (SAP or SDP) that is associated with the service.
Sap Description	The description for the SAP that is associated with the service.
Sdp Systemname	The system name for the SDP bridge that is associated with the service.

Release History

Release 7.3.1; command was introduced.

Related Commands

show service spb ports	Displays the virtual port (SAP and SDP) configuration for the specified service.
show service	Displays the service configuration for the bridge.
show service access	Displays the service access port configuration for the switch.

MIB Objects

N/A

show service spb counters

Displays the traffic statistics for the specified SPB service and associated virtual ports. A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is bound to the specified SPB service.

```
show service spb service_id [sap {port slot/port / linkagg agg_id][:0 | :all | :qtag |
:outer_qtag.inner_qtag] | mesh-sdp sdp_id] counters
```

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
<i>slot/port</i>	The slot and port number of the service access port.
<i>agg_id</i>	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
:qtag	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
:outer_qtag.inner_qtag	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
<i>sdp_id</i>	An existing mesh SDP ID.

Defaults

By default, all statistics counters for the specified service are displayed.

parameter	default
:0 :all :qtag / :outer_qtag.inner_qtag	:0 (null - untagged traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **sap** parameter options with this command to display statistics for a specific SAP ID. A SAP ID is comprised of an access port (*slot/port* or *agg_id*) and an encapsulation value (**:0**, **:all**, **:qtag**, or **:outer_qtag.inner_qtag**) that is used to identify the type of customer traffic to map to the associated service.
- Use the **mesh-sdp** *sdp_id* parameter to display statistics for a specific mesh SDP.

Examples

```
-> show service 100 counters
```

Identifier	Ing Pkts	Ing Byte Counts	Egr Pkts	Egr Byte Counts
sap:1/1:10	1234	12345678	12	123
sap:1/1:15	1234	12345678	12	123
sap:8/2	1234	12345678	12	123
sap:2/3:20.25*	1234	12345678	12	123
sdp:32768:100	34	5678	4321	12345678

```
-> show service 100 sap 1/1:10 counters
```

Identifier	Ing Pkts	Ing Byte Counts	Egr Pkts	Egr Byte Counts
1/1:10	1234	12345678	12	123

```
-> show service 100 mesh-sdp 32768 counters
```

Identifier	Ing Pkts	Ing Byte Counts	Egr Pkts	Egr Byte Counts
32768:100	34	5678	4321	12345678

output definitions

Identifier	The virtual ports (SAPs or SDPs) associated with the service.
Ing Pkts	The number of packets received on the virtual port.
Ing Byte Counts	The ingress packet byte count for the virtual port.
Egr Pkts	The number of packets sent on the virtual port.
Egr Byte Counts	The egress packet byte count for the virtual port.

Release History

Release 7.3.1; command was introduced.

Related Commands

show service	Displays the service configuration for the bridge.
show service spb ports	Displays the virtual ports associated with the specified SPB service.
clear service spb counters	Clears the traffic statistics for the specified SPB service and associated virtual ports.

MIB Objects

alaSapBaseInfoTable
alaSdpBindTable

clear service spb counters

Clears the traffic statistics for the specified SPB service and associated virtual ports. A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is bound to the specified SPB service.

```
clear service spb service_id [sap {port slot/port | linkagg agg_id}][:0 | :all | :qtag |
:outer_qtag.inner_qtag] | mesh-sdp sdp_id] counters
```

Syntax Definitions

<i>service_id</i>	An existing SPB service ID number.
<i>slot/port</i>	The slot and port number of the service access port.
<i>agg_id</i>	The link aggregate ID number (0–31) of a service access link aggregate.
:0	Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
:all	Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
:qtag	Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
:outer_qtag.inner_qtag	Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
<i>sdp_id</i>	An existing mesh SDP ID.

Defaults

By default, all statistics counters for the specified service are cleared.

parameter	default
:0 :all :qtag :outer_qtag.inner_qtag	:0 (null - untagged traffic)

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **sap** parameter options with this command to clear the statistics for a specific SAP ID. A SAP ID is comprised of an access port (*slot/port* or *agg_id*) and an encapsulation value (**:0**, **:all**, **:qtag**, or **:outer_qtag.inner_qtag**) that is used to identify the type of customer traffic to map to the associated service.
- Use the **mesh-sdp** *sdp_id* parameter to clear the statistics for a specific mesh SDP.

Examples

```
-> clear service spb 100 counters
-> clear service spb 100 sap 8/2 counters
-> clear service spb 100 mesh-sdp counters
```

Release History

Release 7.3.1; command was introduced.

Related Commands

[show service spb counters](#) Displays the traffic statistics for the specified SPB service and associated virtual ports.

MIB Objects

```
alaSapBaseInfoTable
alaSdpBindTable
```

45 CMM Commands

The Chassis Management Module (CMM) CLI commands permit you to manage switch software files on the CMM.

MIB information for the CMM commands is as follows:

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

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

A summary of available commands is listed here:

reload secondary
reload slot
reload all
reload from
issu from
write memory
issu slot
copy certified
copy running certified
modify running-directory
copy flash-synchro
takeover
show running-directory
show reload
show microcode
show issu status
usb
usb auto-copy
mount
umount
show usb statistics

reload secondary

Reloads the secondary CMM from the *certified* directory.

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

reload secondary cancel

Syntax Definitions

in [*hours:*] *minutes*

Optional syntax. Schedules a reload of the software to take effect in the time. The time can be specified in 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. See examples below for further explanation.

cancel

Cancels a pending time delayed reboot.

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

- Can be issued from both primary or secondary CMM.
- Reloads the secondary CMM only, the Primary CMM remains operational.

Examples

```
-> reload secondary
-> reload secondary in 15:25
-> reload secondary at 15:25 august 10
-> reload secondary at 15:25 10 august
```

Release History

Release 7.1.1; command introduced.

Related Commands

[reload from](#)

Reloads both CMMs from the specified directory.

MIB Objects

```
chasEntPhysicalTable
  csEntPhysicalIndex
  chasEntPhysAdminStatus
chasControlRedundantTable
  chasControlDelayedRebootTimer
```

reload all

Reloads both Chassis Management Modules (CMMs) from the *certified* directory.

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

reload all cancel

Syntax Definitions

in [*hours:*] *minutes*

Optional syntax. Schedules a reload of all modules to take effect in the specified minutes or hours and minutes within the next 24 hours.

at *hour:minute*

Optional syntax. Schedules a reload of all modules to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is 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 reload.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Can be issued from the Primary CMM only.

Examples

```
-> reload all
-> reload all in 1:30
-> reload all at 12:00 july 25
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload slot Reloads a specific NI module.

MIB Objects

chasEntPhysicalTable

 chasEntPhysAdminStatus

 chasGlobalControl

 chasGlobalControlDelayedResetAll

reload from

Reloads both CMMs from the specified directory. There is no CMM failover during this reboot, causing a loss of switch functionality during the reboot. All the NIs and the secondary CMM will reload.

reload from *image-dir* {**rollback-timeout** *minutes* | **no rollback-timeout** [**in** [*hours:*] *minutes* | **at** *hour:minute*] [**redundancy-time** *minutes*]}

Syntax Definitions

<i>image-dir</i>	The directory that contains the image files to be loaded onto the switch.
rollback-timeout <i>minutes</i>	Sets a timeout period, in minutes. The switch immediately reboots from the specified directory. At the end of this time period, the switch automatically reboots again from the <i>certified</i> directory. The valid range of rollback timeout minutes 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 specified directory until manually rebooted.
in [<i>hours:</i>] <i>minutes</i>	Optional syntax. Schedules a reload of the to take effect in the specified minutes or hours and minutes within the next 24 hours.
at <i>hour:minute</i>	Optional syntax. Schedules a reload 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.
redundancy-time <i>minutes</i>	Specifies the time period in minutes that the switch must run without failure. If a failure occurs within this time period, the switch will reboot from the <i>certified</i> directory.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Can be issued from Primary CMM only.
- This command is used to reload the switch from the specified directory.
- A file verification will be performed before rebooting to ensure all necessary files are present and valid. An error message will be displayed describing any issues found.
- The image directory reload takes place immediately unless a time frame is set using the **in** or **at** keywords.

- If a rollback-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 all** command.
- If the **redundnacy-time** parameter is entered, any reboot of the Primary CMM prior to the redundancy timer expiring will cause the switch to reboot. If the Primary CMM reboots after the redundancy timer expires, the secondary CMM will take over without a reboot.

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 7.1.1; command introduced.

Related Commands

reload all Reboots both CMMs from the *certified* directory.

MIB Objects

```
chasControlModuleTable
  chasControl
  chasControlVersionMngt
  chasControlActivateTimeout
  chasControlRedundancyTime
  chasControlDelayedActivateTimer
  chasControlWorkingVersion
  chasControlNextRunningVersion
```

reload slot

Reloads the NI in the specified slot using the current running image.

reload slot *slot*

Syntax Definitions

slot The slot number to be reloaded.

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

Can be issued from Primary CMM only.

Examples

```
-> reload slot 2
```

Release History

Release 7.1.1; command introduced.

Related Commands

[reload from](#) Reloads both CMMs from the specified directory.

MIB Objects

chasEntPhysicalTable
 chasEntPhysAdminStatus

copy certified

Copies the contents of the *certified* directory to the specified directory.

copy certified *image-dir* [**make-running-directory**]

Syntax Definitions

image-dir

The directory that the contents of the *certified* directory will be copied to.

make-running-directory

Makes the destination directory the new RUNNING DIRECTORY after the configuration is copied.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Using the **make-running-directory** parameter changes the RUNNING DIRECTORY allowing changes to be saved using the **write memory** command.
- This command does not delete any extra files in the target directory.

Examples

```
-> copy certified mydir  
-> copy certified mydir make-running-directory
```

Release History

Release 7.1.1; command introduced.

Related Commands

[copy flash-synchro](#)

Copies the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
chasControlModuleTable  
  chasControlVersionMngt  
  chasControlWorkingVersion
```

issu from

Upgrades the system with the images stored in the specified directory with minimal disruption to traffic.

issu from *image-dir* [**redundancy-time** *minutes*]

Syntax Definitions

image-dir

Specifies the pathname for the directory that contains the image files.

redundancy-time *minutes*

This parameter is not supported with the **issu** command.

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

- The new code must support ISSU with the current running version of code.
- A text file named '*issu_version*' is used to determine ISSU compatibility between code versions. It can be downloaded from the Service and Support website and must be included in the directory along with the new image files.

Examples

```
-> issu from myissu
```

Release History

Release 7.1.1; command introduced.

Related Commands

[issu slot](#)

Causes a power-cycle of the NI in the specified slot after an ISSU upgrade.

MIB Objects

chasEntModuleTable

chasControlWorkingVersion

chasControlRedundancyTime

issu slot

Causes a reset of the NI in the specified slot after an ISSU upgrade.

issu slot *num*

Syntax Definitions

num Specifies the slot number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

Will return an error if ISSU is not in progress or if the slot has already been reset after the ISSU.

Examples

```
-> issu slot 2
```

Release History

Release 7.1.1; command introduced.

Related Commands

[issu from](#) Upgrades the system with the images stored in the specified directory without disruption to traffic.

MIB Objects

chasEntPhysicalTable
entPhysicalIndex

write memory

Copies the current configuration (RAM) to the RUNNING DIRECTORY on the primary CMM.

write memory [**flash-synchro**]

Syntax Definitions

flash-synchro Synchronizes the primary and secondary CMM.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to copy the changes performed using the CLI commands from the running configuration (RAM) to the RUNNING DIRECTORY.
- The **flash-synchro** keyword 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.
- This command is only valid if the switch isn't running from the *certified* directory. Use the [show running-directory](#) command to check where the switch is running from.

Examples

```
-> write memory
-> write memory flash-synchro
```

Release History

Release 7.1.1; command introduced.

Related Commands

[copy flash-synchro](#) Copies the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```
configManager
  configWriteMemory
```

copy running certified

Copies the current *running* directory configuration to the *certified* directory on both CMMs.

copy running certified [flash-synchro]

Syntax Definitions

flash-synchro Synchronizes the primary and secondary CMM.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command is used to overwrite the contents of the *certified* directory with the configuration from the *running* directory. This should only be done if the *running* configuration has been verified.
- The **flash-synchro** keyword 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. In 7.3.1 the flash-synchro functionality is done automatically; entering the **flash-synchro** parameter is no longer required.
- If there is not enough free space, the copy attempt fails and an error message is generated.
- 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.
- This command may take up to two minutes to complete.

Examples

```
-> copy running certified
```

Release History

Release 7.1.1; command introduced.

Release 7.3.1; **flash-synchro** parameter no affect; the functionality is performed automatically.

Related Commands

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

MIB Objects

chasControlModuleTable
chasControlVersionMngt

chasControlWorkingVersion

modify running-directory

Changes the RUNNING DIRECTORY to the specified directory.

modify running-directory *image-dir*

Syntax Definitions

image-dir

The directory name to become the new RUNNING DIRECTORY.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to change the RUNNING DIRECTORY and allow configuration changes to be saved to the new RUNNING DIRECTORY.

Examples

```
-> modify running-directory user-config1  
-> write memory
```

Release History

Release 7.1.1; command introduced.

Related Commands

[write memory](#)

Copies the running primary RAM version of the CMM software to the RUNNING DIRECTORY.

MIB Objects

```
chasControlModuleTable  
    CurrentRunningVersion
```

copy flash-synchro

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

copy flash-synchro

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

- This command is used to synchronize the *certified* directories of the primary and secondary CMMs. The two CMMs must be synchronized if a fail over occurs, otherwise switch performance is affected.

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[copy running certified](#)

Copies the RUNNING DIRECTORY configuration to the *certified* directory on the primary CMM.

MIB Objects

```
chasControlModuleTable
  chasControlVersionMngt
```

takeover

Forces the current secondary CMM to assume the role of the primary CMM.

takeover

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K

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.
- Be sure that the secondary CMM has all software (i.e., image and configuration files) required to continue CMM operations, before issuing the **takeover** command.
- For information on synchronizing the primary and secondary CMM software before issuing the **takeover** command, see the [copy flash-synchro](#) command.

Examples

```
-> takeover
```

Release History

Release 7.1.1; command introduced.

Related Command

[reload all](#) Reboots the switch.

MIB Objects

chasEntPhysicalTable
chasEntPhysAdminStatus

show running-directory

Shows the current state of version and configuration management for a CMM.

show running-directory

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Once a switch boots up and is running, it runs either from the *working*, *certified*, or a *user-defined* directory. If the switch is running from the *certified* directory, changes made to the RUNNING CONFIGURATION using CLI commands, cannot be saved.
- Depending on the switch configuration there may be a small delay before the information is displayed.

Examples

The following is an example of the display on OmniSwitch 10K switches:

```
-> show running-directory
```

```
CONFIGURATION STATUS
  Running CMM           : PRIMARY,
  CMM Mode              : MONO CMM,
  Current CMM Slot     : A,
  Running configuration : CERTIFIED,
  Certify/Restore Status : CERTIFIED,
SYNCHRONIZATION STATUS
  Flash Between CMMs   : SYNCHRONIZED
  Running Configuration : SYNCHRONIZED
```

output definitions

Running CMM	The CMM currently controlling the switch, either PRIMARY or SECONDARY.
CMM Mode	Whether there are one or two CMMs installed.
Current CMM Slot	The slot of the primary CMM, A or B.
Running Configuration	The current RUNNING DIRECTORY.
Certify/Restore Status	Indicates if the CMM has been certified.

output definitions (continued)

Flash Between CMMs	SYNCHRONIZED: Flash between CMMs is identical. NOT SYNCHRONIZED: Flash between CMMs is not identical.
Running Configuration	SYNCHRONIZED: RUNNING CONFIGURATION has been saved to the RUNNING DIRECTORY. NOT SYNCHRONIZED: RUNNING CONFIGURATION has not been saved to the RUNNING DIRECTORY.

Release History

Release 7.1.1; command introduced.

Related Commands

reload all	Reboots the switch.
copy flash-synchro	Copies the <i>certified</i> directory version of the primary CMM software to the <i>certified</i> directory of the secondary CMM.

MIB Objects

```
chasControlModuleTable
  chasControlSynchronizationStatus
  chasControlCertifyStatus
  chasControlRunningVersion
```

```
chasEntPhysicalTable
  chasEntPhysOperStatus
  entPhysicalIndex
```

```
chasControlReloadTable
  chasControlReloadStatus
```

show reload

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

show reload [**status** | **all status**]

Syntax Definitions

status Displays whether or not either of the CMMs are scheduled for a reload.

all status Displays whether or all the modules are scheduled for a reload

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 is going to occur.
- If the **reload from** command is used, and a rollback timeout is set, the rollback occurs and is shown using the **show reload** command.

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[reload secondary](#) Reboots the primary or secondary CMM to its startup software configuration.

[reload from](#) Immediate primary CMM reboot to the specified software configuration without secondary CMM takeover.

MIB Objects

```
chasControlModuleTable
  chasControlDelayedActivateTimer
chasGlobalControl
  chasGlobalControlDelayedResetAll
```

show microcode

Displays microcode versions installed on the switch.

show microcode [**certified** | **loaded** | **issu** | *image-dir*]

Syntax Definitions

certified	Specifies the <i>certified</i> directory.
loaded	Specifies the loaded (i.e., currently-active) microcode versions.
working	Specifies the <i>working</i> directory.
issu	Specifies the <i>issu</i> directory.
<i>image-dir</i>	Specifies the <i>user-defined</i> directory.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If no additional parameters are entered microcode information for the RUNNING CONFIGURATION is displayed.

Examples

```
-> show microcode
Package           Release           Size           Description
-----+-----+-----+-----
Ros.img           7.1.1.403.R01    1828255       Alcatel-Lucent OS
Reni.img          7.1.1.403.R01    1359435       Alcatel-Lucent NI
```

output definitions

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

Release History

Release 7.1.1; command introduced.

Related Commands

usb Displays the archive history for 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 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

MIB Objects

usb auto-copy

Allows backup image files from the USB device to be automatically copied to the /flash/working directory on the switch immediately after the USB device is connected

MIB Objects

```
systemServices
  systemServicesUsbEnable
```

usb auto-copy

Allows the image files from the USB device to be automatically copied to 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 10K, 6900

Usage Guidelines

- If the auto-copy is successful the switch will automatically reboot.
- The USB device must contain the proper file structure and image files mentioned below and the USB root directory must contain a signature file named *aossignature*. The *aossignature* file can be a blank text file transferred to the switch.
- This operation will enable all of the image files from the */uflash/10000/working* or */uflash/6900/working* directory to be copied to the */flash/working* directory.
- If the auto-copy is successful, the auto-copy feature will be disabled before rebooting the switch and must be re-enabled by the administrator for the next auto-copy process to execute. This will prevent running the same auto-copy multiple times.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands**usb**

Enables access to the device connected to the USB interface.

MIB Objects

systemServices

systemServicesUsbAutoCopyEnable

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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

umount Unmounts the /uflash file system from AOS.

MIB Objects

```
systemServicesAction  
  systemServicesArg1
```

umount

Unmounts the /uflash file system from AOS.

umount /uflash

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

```
-> umount /uflash
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[mount](#) Mounts the /uflash file system from AOS.

MIB Objects

```
systemServicesAction  
systemServicesArg1
```

show usb statistics

Displays the status USB setting and features.

show usb statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show usb statistics
Filesystem          1K-blocks      Used Available Use% Mounted on
/dev/sdb1           500732         261216    239516   52% /vroot/uflash
  Host scsi6: usb-storage
    Vendor: Alcatel-Lucent
    Product: USB
  Serial Number: AA04012700031693
    Protocol: Transparent SCSI
    Transport: Bulk
      usb: enabled
usb auto-copy: disable
auto-copy in progress: No
```

output definitions

usb	Status of USB device interface.
usb auto-copy	Status of USB auto-copy feature.
auto-copy in progress	Is the switch currently in the process of performing an auto-upgrade.

Release History

Release 7.1.1; command was introduced.

Related Commands

usb	Enables access to the device connected to the USB interface.
usb auto-copy	Allows backup files from the USB device to be automatically copied to the switch immediately after the USB device is connected.
mount	Mounts the /uflash file system.

MIB Objects

```
systemServices
  systemServicesUsbEnable
  systemServicesUsbAutoCopyEnable
  systemServicesUsbDisasterRecoveryEnable
```

show issu status

Displays the status of ISSU.

show issu status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

N/A

Examples

```
-> show issu status
Slot      ISSU-Status
-----+-----+
 1         ISSU Pending
 2         ISSU Pending
 3         ISSU Pending

-> show issu status
Slot      ISSU-Status
-----+-----+
 1         ISSU Complete
 2         ISSU Complete
 3         ISSU Complete
```

output definitions

Slot	Specifies the slot number.
ISSU-Status	Indicates the ISSU status for a slot: Pending - Slot has not been reset; upgrade is not complete. Complete - Slot has been reset; upgrade is complete.

Release History

Release 7.1.1; command was introduced.

Related Commands**issu from**

Upgrades the system with the images stored in the specified directory without disruption to traffic.

MIB Objects

N/A

46 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

A summary of available commands is listed here:

Management Commands	<code>system contact</code> <code>system name</code> <code>system location</code> <code>system date</code> <code>system time</code> <code>system timezone</code> <code>system daylight-savings-time</code> <code>update uboot</code> <code>update fpga</code> <code>reload slot</code> <code>power slot</code> <code>temp-threshold</code> <code>powersupply enable</code> <code>powersupply powersave</code> <code>hash-control</code>
Monitoring Commands	<code>license</code> <code>show hardware-info</code> <code>show chassis</code> <code>show cmm</code> <code>show slot</code> <code>show module</code> <code>show module long</code> <code>show module status</code> <code>show powersupply</code> <code>show fan</code> <code>show fantray</code> <code>show temperature</code> <code>show hash-control</code>
Licensing Commands	<code>license</code> <code>show license-info</code>

system contact

Specifies the administrative contact for 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 10K, 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

system name	Modifies the current system name of the switch.
system location	Specifies the current physical location of the switch.
license	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 19 characters in length. No spaces are allowed in the system name.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Spaces are not allowed in the system name.

Examples

```
-> system name OmniSwitch10K
-> system name OS10K
```

Release History

Release 7.1.1; command introduced.

Related Commands

[system contact](#)

Specifies the administrative contact of the switch (for example, an individual or a department).

[system location](#)

Specifies the current physical location of the switch.

[license](#)

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 very 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 10K, 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; 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.

[license](#)

Displays the basic system information for the switch.

MIB Objects

system

 systemLocation

system date

Displays or modifies the current system date on 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 10K, 6900

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 46-8.

Examples

```
-> system date 08/08/2010
-> system date
08/08/2010
```

Release History

Release 7.1.1; command introduced.

Related Commands

[system time](#)

Displays or modifies the current system time on the switch.

[system timezone](#)

Displays or modifies the time zone for the switch.

MIB Objects

systemServices

systemServicesDate

system time

Displays or modifies the switch current system time.

system time [*hh:mm:ss*]

Syntax Definitions

hh:mm:ss

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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
-> system time
14:30:08
```

Release History

Release 7.1.1; command introduced.

Related Commands

[system date](#)

Displays or modifies the current system date on the switch.

[system timezone](#)

Displays or modifies the time zone for the switch.

MIB Objects

systemServices

systemServicesTime

system timezone

Displays or modifies the time zone for the switch.

system timezone [*timezone_abbrev*]

Syntax Definitions

timezone_abbrev

Specifies a time zone for the switch and sets the system clock to run on UTC. If you specify a time zone abbreviation, the hours offset from UTC is automatically calculated by the switch.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The configuration must be saved after changing the timezone.
- To display the current time zone for the switch, enter the syntax **system timezone**.
- If the configured timezone supports DST it is automatically enabled and cannot be disabled.
- If the configured timezone does not support DST it is automatically disabled and cannot be enabled.
- Refer to the Switch Management Guide for a list of time zone abbreviations.

Examples

```
-> system timezone mst
```

Release History

Release 7.1.1; command introduced.

Related Commands

[system date](#)

Displays or modifies the current system date on the switch.

[system time](#)

Displays or modifies the current system time on the switch.

MIB Objects

systemServices

```
systemServicesTimezone  
systemServicesTimezoneStartWeek  
systemServicesTimezoneStartDay  
systemServicesTimezoneStartMonth  
systemServicesTimezoneStartTime
```

```
systemServicesTimezoneOffset  
systemServicesTimezoneEndWeek  
systemServicesTimezoneEndDay  
systemServicesTimezoneEndMonth  
systemServicesTimezoneEndTime  
systemServicesEnabledDST
```

system daylight-savings-time

Displays the Daylight Savings Time (DST) setting for the configured timezone.

system daylight-savings-time

Syntax Definitions

N/A

Defaults

parameter	default
Timezone supports DST	enabled
Timezone does not support DST	disabled

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the configured timezone supports DST it is automatically enabled and cannot be disabled.
- If the configured timezone does not support DST it is automatically disabled and cannot be enabled.
- DST will always display as ENABLED, the configured timezone determines its operation.

Examples

```
-> system daylight-savings-time
Daylight Savings Time (DST) is ENABLED.
```

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

```
systemServices
  systemServicesTimezone
  systemServicesEnabledDST
```

update uboot

Updates the uboot versions of the CMM or NIs. Refer to the Release Notes and/or any available Upgrade Instructions for the new release before performing this type of update on the switch.

update uboot {cmm *slot* | ni {all | *slot*} file *filename*}

Syntax Definitions

cmm	Specifies that the update is performed for the Chassis Management Module (CMM).
all	Specifies that the update is performed for all slots within a chassis.
<i>slot</i>	Specifies the slot number of the module within a chassis.
<i>filename</i>	Specifies the path and name of the upgrade file.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Note that when performing an update, it is important that the correct update file is used. Specifying the wrong file may impact the operation of the switch.

Examples

```
OS10K-> update uboot ni all file 9999.tar.gz
OS10K-> update uboot cmm 1 file /flash/temp/9999.tar.gz
```

Release History

Release 7.1.1; command introduced.

Related Commands

reload slot Reloads the specified NI module.

MIB Objects

```
systemServices
  systemServicesArg1
  systemServicesAction
```

update fpga

Updates the fpga versions of the CMM or NIs. Refer to the Release Notes and/or any available Upgrade Instructions for the new release before performing this type of update on the switch.

```
update fpga {cmm slot| ni {daughter | slot } file filename}
```

Syntax Definitions

cmm	Specifies that the update is performed for the Chassis Management Module (CMM).
daughter	Specifies the number of the daughter board on the NI module.
<i>slot</i>	Specifies the slot number of the module within a chassis.
<i>filename</i>	Specifies the path and name of the upgrade file.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Note that when performing an update, it is important that the correct update file is used. Specifying the wrong file may impact the operation of the switch.

Examples

```
OS10K-> update fpga ni 4 file 9999.vme
OS10K-> update fpga cmm 1 file /flash/temp/9999.vme
```

Release History

Release 7.1.1; command introduced.

Related Commands

[reload slot](#) Reloads the specified NI module.

MIB Objects

```
systemServices
  systemServicesArg1
  systemServicesAction
```

reload slot

Reloads or reboots a specified Network Interface (NI) module.

reload slot *slot*

Syntax Definitions

slot Specifies the slot number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The **reload slot** command reboots only the specified NI. Other modules installed on the chassis, including primary and secondary CMMs, are not affected

Examples

```
-> reload slot 2
```

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

```
chasEntPhysicalTable  
  chasEntPhysAdminStatus  
  reset
```

power slot

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

power slot *slot*

no power slot *slot*

Syntax Definitions

slot The chassis slot number containing the NI module being powered on or off.

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

Use the **no** form of this command to power off an NI module.

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[reload slot](#) Reloads the specified NI module.

[show slot](#) Shows the hardware information and current status for Network Interface (NI) modules currently running in the chassis.

MIB Objects

```
chasEntPhysicalTable  
  chasEntPhysAdminStatus  
  powerOn  
  powerOff
```

temp-threshold

Sets the warning temperature threshold for the switch.

temp-threshold *temp*

Syntax Definitions

temp The new temperature threshold value, in Celsius.

Defaults

parameter	default
<i>temp</i>	67 (OS6900)

Platforms Supported

OmniSwitch 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; command introduced.

Release 7.3.1; command deprecated.

Related Commands

[show temperature](#) Displays the ambient temperature of the current operating chassis, as well as current temperature threshold settings.

MIB Objects

chasChassisTable
 chasTempThreshold

powersupply enable

Enables the power supply unit identified by the PSU-ID.

powersupply enable [*slot*]

no powersupply enable [*slot*]

Syntax Definitions

slot Slot number of power supply.

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

N/A

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

N/A

powersupply powersave

Enables the power saving functionality on the switch.

powersupply powersave {enable | disable}

Syntax Definitions

enable | disable Enables or disables the power saving functionality.

Defaults

parameter	default
enable disable	enable

Platforms Supported

OmniSwitch 10K

Usage Guidelines

- When enabled unneeded power-supplies are shut down to conserve energy, only the power supplies required to provide N+1 redundancy remain on.
- If enabled and power is lost to all active power supplies simultaneously the switch will lose power since N+1 redundancy applies only to the active power supplies.
- If the power-save mode is disabled, all available power supplies are switched on at all times.

Release History

Release 7.1.1; command introduced.

Related Commands

show powersupply Displays the hardware information and current status for chassis power supplies.

MIB Objects

chasEntPhysicalTable
 chasEntPhysAdminStatus

hash-control

Configures the hash control method on the switch. Depending upon this configuration, hashing algorithm used by various applications for packet forwarding is affected.

hash-control {brief | extended [udp-tcp-port] | load-balance non-ucast {enable | disable}}

hash-control extended no udp-tcp-port

Syntax Definitions

brief	Sets hashing to brief mode.
extended	Sets hashing to extended mode.
udp-tcp-port	Sets extending hashing to use UDP/TCP ports.
enable disable	Enables or disables the the load balancing of non-unicast traffic on a link aggregate.

Defaults

parameter	default
hash-control	brief
udp-tcp-port	disabled
non-ucast	disabled

Platforms Supported

OmniSwitch 6900

Usage Guidelines

- Disabling TCP-UDP port hashing is recommended when Server Load Balancing (SLB) is configured, because SLB dynamically assigns ports.
- The hash control setting also impacts the fabric load balancing for Chassis based products. It is recommended not to set brief hashing mode on Chassis based products.
- Changing the hash control mode affects the hashing algorithm for Link Aggregation, Server Load Balancing and ECMP.
- The hashing mode must be set to extended to enable UDP/TCP port hashing.
- Enabling or disabling the **load-balance non-ucast** option applies to all link aggregates. When this option is disabled (the default), link aggregation load balances only unicast packets; all non-unicast packets are sent through the primary port of the link aggregate.
- When the **load-balance non-ucast** option is enabled, all non-unicast traffic (broadcast, L2 multicast, L3 multicast, and unknown unicast) is load balanced over the link aggregate.

Examples

```
-> hash-control brief
-> hash-control extended
-> hash-control extended udp-tcp-port
-> hash-control extended no udp-tcp-port
-> hash-control load-balance non-ucast enable
-> hash-control load-balance non-ucast disable
```

Release History

Release 7.2.1; command introduced.

Related Commands

[show hash-control](#) Displays the current hash control setting for the switch.

MIB Objects

```
alaChasHashMode
alaChasUdpTcpPortMode
alachasNonUHashControl
```

license

Activates the license for licensed protocols on the switch.

license apply file *file_name*

Syntax Definitions

file_name *The name of the license file containing the license keys.*

Defaults

By default licensed protocols are not activated on the switch.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The license file can have any name.
- The license file is only used to activate the licensed features and does not need to remain on the switch.
- The switch must be rebooted to reflect the licensed feature set.

Examples

```
-> license apply file /flash/swlicense.dat
The switch will reboot after the license is applied.
Are you sure you want to proceed(Y/N)?Y
```

Release History

Release 7.2.1; command was introduced.
Release 7.3.1; **key** and **deactivate** parameters deprecated.

Related Commands

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

MIB Objects

alaCapManVcSwLicensingAction
 alaCapManSwLicensingActionArg

show system

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

show system

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show system
System:
```

```
Description: Alcatel-Lucent OS10K 7.1.1.999, February 21, 2010.,
Object ID: 1.3.6.1.4.1.6486.800.1.1.2.1.6.1.2,
Up Time: 0 days 5 hours 20 minutes and 49 seconds,
Contact: Alcatel-Lucent, www.alcatel-lucent.com/enterprise/en,
Name: OmniSwitch 10K,
Location: NMS_LABORATORY,
Services: 72,
Date & Time: FRI FEB 24 2006 16:21:30 (PST)
```

```
Flash Space:
```

```
Primary CMM:
Available (bytes): 31266816,
Comments : None
```

output definitions

System Description	The description for the current system. This description shows the current software version and the system date.
System Object ID	The SNMP object identifier for the switch.
System Up Time	The amount of time the switch has been running since the last system reboot.
System Contact	An user-defined administrative contact for the switch. This field is modified using the system contact command.
System Name	A user-defined text description for the switch. This field is modified using the system name command.

output definitions (continued)

System Location	The user-defined physical location of the switch. This field is modified using the system location command.
System Services	The number of current system services.
System Date & Time	The current system date and time. This field is modified using the system date and system time commands.
Flash Space: Primary CMM: Available (bytes)	The available flash memory space available on the <i>primary</i> 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 7.1.1; command introduced.

Related Commands

system contact	Specifies the administrative contact for 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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show hardware-info
CPU Type                : PowerPC 8245,
Flash Manufacturer      : TOSHIBA,
Flash size              : 67108864 bytes (64 MB),
RAM Manufacturer        : (null),
RAM size                : 268435456 bytes (256 MB),
NVRAM Battery OK ?     : YES,
BootROM Version         : 6.1.2.20.R02 ,
Backup Miniboot Version : 6.1.2.20.R02,
Default Miniboot Version : 6.1.2.20.R02,
Product ID Register     : 54
Hardware Revision Register : 00
CPLD Revision Register  : 06
XFP Module ID           : 02
```

output definitions

CPU Type	The manufacturer and model number of the CPU used on the CMM.
Flash Manufacturer	The manufacturer of the flash memory used on the CMM.
Flash size	The total amount of flash memory (file space) on the CMM. This field specifies the total flash memory size only and does not indicate the amount of memory free or memory used.
RAM Manufacturer	The manufacturer of the RAM memory used on the CMM.
RAM size	The total amount of RAM memory on the CMM. This field specifies the total RAM memory only and does not indicate the amount of memory free or memory used.

output definitions (continued)

NVRAM Battery OK	The current status of the NVRAM battery. If the battery is OK, YES is displayed in this field. If the battery charge becomes low, NO is displayed in this field.
BootROM Version	The current BootROM version.
Backup Miniboot Version	The current backup miniboot version.
Default Miniboot Version	The current default miniboot version.
Product ID Register	The register number of the product ID.
Hardware Revision Register	The register number of the hardware revision.
CPLD Revision Register	The register number of the CPLD revision.
XFP Module ID	The ID number of the XFP module.

Release History

Release 7.1.1; 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

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

-> show chassis

```
Chassis 1
  Model Name:           OS10K,
  Description:          Chassis,
  Part Number:          902274-10,
  Hardware Revision:    002,
  Serial Number:        E23L9052,
  Manufacture Date:     JUN 09 2004,
  Admin Status:         POWER ON,
  Operational Status:   UP,
  Free Slots:           5,
  Power Left:           200,
  Number Of Resets:     115,
  MAC Address           00:d0:95:87:14:33
```

output definitions

Model Name	The factory-set model name for the switch. This field cannot be modified.
Description	The factory-set description for the switch. This field cannot be modified.
Part Number	The Alcatel-Lucent part number for the chassis.
Hardware Revision	The hardware revision level for the chassis.
Serial Number	The Alcatel-Lucent serial number for the chassis.
Manufacture Date	The date the chassis was manufactured.

output definitions (continued)

Admin Status	The current power status of the chassis. Chassis information is obtained from a running CMM. Hence the value is always POWER ON.
Operational Status	The current operational status of the chassis.
Free Slots	The number of free slots available for NIs.
Power Left	The power remaining for additional NIs.
Number of Resets	The number of times the CMM has been reset (reloaded or rebooted) since the last cold boot of the switch.
MAC Address	The base MAC address of the chassis.

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

```
chasChassisTable
  chasFreeSlots
  chasPowerLeft
```

show cmm

Displays basic hardware and status information for the CMM modules in a standalone switch.

show cmm [*slot*]

Syntax Definitions

slot Specifies the CMM by slot number or letter.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

On chassis-based switches, a CMM installed in the left CMM slot position is defined as CMM-A. A CMM installed in the right position is CMM-B.

```
-> show cmm 1
Module in slot CMM-A
  Model Name:           OS10K,
  Description:          CMM,
  Part Number:          902271-10,
  Hardware Revision:    002,
  Serial Number:        E23L9059,
  Manufacture Date:     JUN 08 2004,
  FPGA Physical-1:     December 24 2009,
  Admin Status:         POWER ON,
  Operational Status:   UP,
  Power Consumption:    888,
  CPU Model:            MPC8572 Motorola,
  MAC Address:          00:d0:95:a3:e5:09,
```

output definitions

Model Name	The model name of the switch. Note that on chassis-based switches, CMM modules are made up of two major subcomponents: the fabric board and the processor board. Fabric boards are denoted as OS10*00-CMM and processor boards are denoted as CMM-PROC. Information for each board is displayed separately.
Description	A factory-defined description of the associated board (for example, BBUS Bridge or PROCESSOR).
Part Number	The Alcatel-Lucent part number for the board.
Hardware Revision	The hardware revision level for the board.
Serial Number	The Alcatel-Lucent serial number for the board.
Manufacture Date	The date the board was manufactured.
FPGA Physical-1	FPGA version.

output definitions (continued)

Admin Status	The current power status of the CMM. Information is obtained from a running CMM. Hence the value is always POWER ON.
Operational Status	The current operational status of the CMM.
Power Consumption	The current power consumption for the CMM.
CPU Model	The CPU Model type.
MAC Address	The MAC address assigned to the chassis.

Release History

Release 7.1.1; command introduced.

Related Commands

show chassis	Displays the basic configuration and status information for the switch chassis.
show slot	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.
license	Displays the status and configuration of Switch Fabric Modules (SFMs) on chassis-based switches.

MIB Objects

N/A

show slot

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

show slot [*slot*]

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When this command is entered from the secondary CMM, the Operational and Admin Status for NIs will display as 'UNKNOWN'.

Examples

```
-> show slot 1
Module in slot 1
  Model Name:                OS10-GNI-C48,
  Description:               10-1000 RJ45,
  Part Number:              902434-90,
  Hardware Revision:        A07,
  Serial Number:            H03Q0008,
  Manufacture Date:         JAN 31 2007,
  FPGA - Physical 1:        007,
  Daughter FPGA - Physical 1: 002,
  Daughter FPGA - Physical 2: 002,
  Admin Status:             POWER ON,
  Operational Status:       UP,
  Power Consumption:        200,
  CPU Model Type   :        Motorola MPC854
  MAC Address:            00:d0:95:01:04:
  ASIC - Physical 1:        BCM56620_A1,
  ASIC - Physical 2:        BCM56620_A1,
  ASIC - Physical 3:        BCM56620_A1,
  ASIC - Physical 4:        BCM56620_A1,
  ASIC - Physical 5:        BCM56620_A1,
  ASIC - Physical 6:        BCM56620_A1,
  UBOOT Version:          7.1.1.412.R01,
```

output definitions

Model Name	The NI module name. For example, OS9-GNI-C24 indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Description	A general description of the NI. For example, 24pt 10/100/1000BaseT Mod indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Part Number	The Alcatel-Lucent part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The Alcatel-Lucent serial number for the NI printed circuit board (PCB).
Manufacture Date	The date the NI was manufactured.
FPGA/Daughter FPGA	The FPGA versions.
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 module.
CPU Model Type	The CPU model type.
MAC Address	The MAC address assigned to the NI.
ASIC - Physical	General information regarding the NI module ASICs.
UBOOT Version	UBOOT version of the NI.

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

chasEntPhysOperStatus

show module

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

show module [*slot*]

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

-> show module

Slot	Part-Number	Serial #	HW Rev	Mfg Date	Model Name
CMM-A	902271-10	E23L9059	002	JUN 08 2004	OS10-CPM
SLOT-1	902271-10	E23L9059	002	JUN 08 2004	OS10-GNI-C48

output definitions

Slot	The chassis slot position of the module.
Part-Number	The Alcatel-Lucent part number for the module.
Serial #	The Alcatel-Lucent serial number for the module.
Rev	The hardware revision level for the module.
Date	The date the module was manufactured.
Model Name	The descriptive name for the module.

Release History

Release 7.1.1; 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.

show module long [*slot*]

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show module long 1
Module in slot 1
  Model Name:                OS10-GNI-C48,
  Description:                10-1000 RJ45,
  Part Number:                902434-90,
  Hardware Revision:          A07,
  Serial Number:              H03Q0008,
  Manufacture Date:           JAN 31 2007,
  FPGA - Physical 1:          007,
  Daughter FPGA - Physical 1: 002,
  Daughter FPGA - Physical 2: 002,
  Admin Status:               POWER ON,
  Operational Status:         UP,
  Power Consumption:          200,
  CPU Model Type   :          Motorola MPC854
  MAC Address:                00:d0:95:01:04:
  ASIC - Physical 1:          BCM56620_A1,
  ASIC - Physical 2:          BCM56620_A1,
  ASIC - Physical 3:          BCM56620_A1,
  ASIC - Physical 4:          BCM56620_A1,
  ASIC - Physical 5:          BCM56620_A1,
  ASIC - Physical 6:          BCM56620_A1,
  UBOOT Version:              7.1.1.412.R01,
```

output definitions

Model Name	The NI module name. For example, OS9-GNI-C24 indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Description	A general description of the NI. For example, 24pt 10/100/1000BaseT Mod indicates a twenty four-port 10/100/1000BaseT Ethernet module.
Part Number	The Alcatel-Lucent part number for the NI.
Hardware Revision	The hardware revision level for the NI.
Serial Number	The Alcatel-Lucent serial number for the NI printed circuit board (PCB).
Manufacture Date	The date the NI was manufactured.
FPGA/Daughter FPGA	The FPGA versions.
Admin Status	The current power status of the module. Options include POWER ON or POWER OFF.
Operational Status	The operational status of the module. 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 module.
CPU Model Type	The CPU model type.
MAC Address	The MAC address assigned to the module.
ASIC - Physical	General information regarding the module ASICs.
UBOOT Version	UBOOT version of the module.

Release History

Release 7.1.1; 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.

show module status [*slot*]

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

When this command is entered from the secondary CMM, the Operational and Admin Status for NIs will display as 'UNKNOWN'.

Examples

```
-> show module status
      Operational          Firmware
Slot   Status      Admin-Status  Rev      MAC
-----+-----+-----+-----+-----
CMM-A   UP           POWER ON     N/A     00:d0:95:a3:e5:09
SLOT-1  UP           POWER ON     N/A     00:d0:95:a3:e5:0b
```

output definitions

Slot	The chassis slot position of the module. For detailed slot numbering information, refer to the “Chassis and Power Supplies” chapter of the <i>Hardware User Guide</i> . Refer to page 46-27 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.
Firmware Rev	The firmware version for module ASICs.
MAC	For the CMM, the base chassis MAC address is displayed. For NI modules, the MAC address for the corresponding NI is displayed.

Release History

Release 7.1.1; 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 powersupply

Displays the hardware information and current status for chassis power supplies.

show powersupply [*slot*] [**powersave status**]

Syntax Definitions

slot The slot number for a specific power supply installed in the chassis. If no power supply number is specified, information for all power supplies is displayed.

powersave status Displays the status of the power saving functionality.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Power supplies 5-8 are for the optional power supply shelf on OS10K.
- The power-save feature is only supported on the OS10K.

Examples

```
-> show powersupply
```

Slot	PS	Total Power	Power Used	Input Voltage	PS Type	Status	Location
1		2400	0	0	AC	UP	Internal
2		2400	0	0	AC	UNPLUG	Internal
3		2400	564	226	AC	UP	Internal
4		2400	504	226	AC	UP	Internal
5		--	--	--	--	--	--
6		--	--	--	--	--	--
7		--	--	--	--	--	--
8		--	--	--	--	--	--

```
-> show powersupply
```

Slot	PS	Total Power	Power Used	PS Type	Status	Location	Airflow
1		450	201	AC	UP	Internal	Front to Rear
2		450	50	AC	UP	Internal	Front to Rear

```
-> show powersupply 1
```

```
Module in slot PS-1
Model Name:          YM-2451DDR,
Module Type:         DC/DC Power Supply, Front to Rear Airflow
Description:         OS-PS-450W-D
Hardware Revision:   B0,
Serial Number:       1020000417,
Manufacture Date:    May 14 2010,
Operational Status: UP,
Power Provision:     450W
```

output definitions

Model Name	The power supply model number.
Description	A description of the associated power supply. This field reflects the model name in most cases.
Part Number	The Alcatel-Lucent part number for the power supply.
Hardware Revision	The hardware revision level for the power supply.
Serial Number	The Alcatel-Lucent serial number for the power supply.
Manufacture Date	The date the power supply was manufactured.
Operational Status	The operational status of the power supply. Options include UP or DOWN.
Power Provision	The number of watts provided by this power supply.
PS	The slot number of the power supply.
Total Power	The number of watts provided by this power supply.
Power Used	The number of watts being used by this power supply.
Input Voltage	The input line voltage of this power supply.
PS type	The type of power supply. AC or DC.
Operational Status	The operational status of the power supply. Options include UP, DOWN, or UNPLUG.
Location	The location of the power supply. Options include Internal or External. Slots 5-8 are for the optional power shelf.
Airflow	Direction of airflow.

Release History

Release 7.1.1; 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 [*slot*]

Syntax Definitions

slot Specifies the slot number of the fantray.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guideline

N/A

Examples

```
-> show fan
Chassis Fan  Status
-----+-----
  1      1  Running
  1      2  Running
  1      3  Running
  1      4  Not Running
```

output definitions

Chassis/Tray	The chassis/tray ID.
Fan	The fan number describing the fan position.
Status/Functional	The current operational status of the corresponding fan.
Speed	The speed of the fan.
Airflow	-

Release History

Release 7.1.1; command introduced.

Related Commands**show fantray**

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

MIB Objects

N/A

show fantray

Displays the current operating status of chassis fantrays.

show fantray [*slot*]

Syntax Definitions

slot Specifies the slot number of the fantray.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guideline

N/A

Examples

```
-> show fantray
      | Working | Fan
Tray | Status | Fans  | Load %
-----+-----+-----+-----
  1   ON   4     50
```

output definitions

Chassis/Tray	The chassis/Tray ID.
Status	The current operational status of the fantray.
Working Fans	The number of working fans.
Fan Load %	The load of the fantray.

Release History

Release 7.1.1; command introduced.

Related Commands

[show fantray](#) Displays the current operating chassis ambient temperature, as well as current temperature threshold settings.

MIB Objects

N/A

show temperature

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

show temperature [**fabric** *[index]*] | **slot** *[index]*] | **fantray** *[index]*] | **cmm** *[index | cmm_letter]*]

Syntax Definitions

index Specifies the index number.

number Specifies the slot number.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show temperature
Device | Current | Range | Thresh | Status
-----+-----+-----+-----+-----
CMM    | 45      | 15-60 | 55     | UNDER THRESHOLD
FAB1   | 46      | 15-60 | 55     | UNDER THRESHOLD
Slot1  | 43      | 15-60 | 55     | UNDER THRESHOLD
Slot3  | 43      | 15-60 | 55     | UNDER THRESHOLD
Slot4  | 43      | 15-60 | 55     | UNDER THRESHOLD
```

output definitions

Device	The device being measured (CMM, Fabric, or NI)
Current	The current CPU temperature in Celsius.
Range	The supported threshold range.
Thresh	The warning temperature threshold, in degrees Celsius. If the switch reaches or exceeds this temperature, the primary switch or CMM TEMP LED displays amber and a warning is sent to the user.
Status	Whether the current temperature has reached the threshold.

Release History

Release 7.1.1; command introduced.

Related Commands

[temp-threshold](#)

Sets the chassis warning temperature threshold.

[show fan](#)

Shows the hardware information and current status for the chassis fans.

MIB Objects

chasChassisTable

 chasHardwareBoardTemp

 chasHardwareCpuTemp

 chasTempRange

 chasTempThreshold

 chasDangerTempThreshold

show hash-control

Displays the current hash control settings for the switch.

show hash-control [non-ucast]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6900

Usage Guidelines

N/A

Examples

```
-> show hash-control

Hash Mode      = brief,
Udp-Tcp-Port  = disabled
-> show hash-control non-ucast
Hash Status = Enabled,
Hash Mode : Normal
```

output definitions

Hash Mode	The current Hash Mode.
Udp-Tcp-Port	Status of UDP/TCP hashing.
Non-ucast Hash Status	Status of Non-ucast Hash status.

Release History

Release 7.2.1; command introduced.

Related Commands

[powersupply powersave](#) Configures the hash mode of the switch..

MIB Objects

```
alaChasHashMode
alaChasUdpTcpPortMode
alachasNonUHashControl
```

show license-info

Displays all the licensed applications installed on the switch.

show license-info

Syntax Definitions

NA

Defaults

NA

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to verify which licenses are installed on the switch.
- The number of days remaining is only applicable for demo licenses.

Examples

```
->show license-info
```

VC	Device	License	Type	Time (Days) Remaining
0	0	Advanced	Permanent	NA

output definitions

VC	Virtual chassis identifier.
Device	Slot number of NI.
License	Displays the feature license installed on the switch. Advanced, Data Center, U16L
Type	The type of license: Demo or Permanent.
Time (Days) Remaining	Time of days remaining for a demo license. Display as 'NA' for permanent licenses.

Release History

Release 7.2.1; command was introduced.

Related Commands

license Activates the license for licensed protocols on the switch.

MIB Objects

```
alaVcCapManSwLicensingInfoTable  
  alaVcLicensedvcSlot  
  alaVcLicensedMask  
  alaVcLicenseType  
  alaVcTimeRemain
```

47 Chassis MAC Server (CMS) Commands

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

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

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

The MAC address range is stored on the switch's EEPROM. The switch supports one MAC address range only. By default, this MAC address range contains thirty-two (32) factory-installed, contiguous MAC addresses.

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

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

A summary of the available commands is listed here:

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

mac-range eeprom

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

Note. Use caution when modifying the default MAC range. Improper use of this command can disable your system and adversely affect your network. Contact Alcatel-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 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command introduced.

Related Commands

[show mac-range](#)

Displays the MAC range table.

MIB Objects

chasMacAddressRangeTable

 chasMacRangeIndex

 chasGlobalLocal

 chasMacAddressStart

 chasMacAddressCount

show mac-range

Displays the MAC range table.

show mac-range [*index*]

Syntax Definitions

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

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

```
-> show mac range
```

Mac Range	Row Status	Local/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 <i>EEPROM</i> 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 7.1.1; command 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 10K, 6900

Usage Guidelines

N/A.

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 47-4 for more information.
Mac Address	Current MAC address allocated for a specific application.

output definitions (continued)

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

Release History

Release 7.1.1; command introduced.

Related Commands

[mac-range eeprom](#) Modifies the default MAC range on the switch's EEPROM.

MIB Objects

ChasMacAddressAllocTable
 chasAppId
 chasObjectId
 chasAllocMacRangeIndex
 chasAllocMacAddress

48 Network Time Protocol Commands

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

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

The MIB information for NTP is as follows:

Filename: AlcatelIND1Ntp.mib
Module: alcatelIND1NTPMIB

A summary of available commands is listed here:

- ntp server**
- ntp server synchronized**
- ntp server unsynchronized**
- ntp client**
- ntp src-ip preferred**
- ntp broadcast**
- ntp broadcast-client**
- ntp broadcast-delay**
- ntp key**
- ntp key load**
- ntp authenticate**
- ntp master**
- ntp interface**
- ntp max-associations**
- ntp broadcast**
- ntp peer**
- ntp vrf-name**
- show ntp status**
- show ntp client**
- show ntp client server-list**
- show ntp server client-list**
- show ntp server status**
- show ntp keys**
- show ntp peers**
- show ntp server disabled-interfaces**

ntp server

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

ntp server {*ip_address*} [**key** *keyid*] [**minpoll** *poll*] [**version** *version*] [**prefer**]

no ntp server {*ip_address*}

Syntax Definitions

<i>ip_address</i>	The IP address of the NTP server to be added or deleted to the client's server list.
<i>key id</i>	The key identification number that corresponds to the specified NTP server. The value ranges from 1 to 65534.
<i>poll</i>	It specifies the minimum polling interval for NTP message. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds ($2^4 = 16$). The maximum poll interval is fixed at 10 (1,024 s). The minimum poll interval defaults to 6 (64 s), but can be decreased by the minpoll option to a lower limit of 4 (16 s), or increase to the maximum limit of 10.
<i>version</i>	The version of NTP being used. This will be 1, 2, 3, or 4.
prefer	Marks this server as the preferred server. A preferred server's timestamp will be used before another server.

Defaults

Parameter	Default
<i>version</i>	4
<i>exponent</i>	6
prefer	not preferred

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the **no** form of this command to clear an NTP server from the list of configured servers.
- To configure NTP in the client mode you must first define the NTP servers. Up to 3 NTP servers may be defined.
- Either an IP address or domain name for the specified server can be entered.
- The NTP key identification is an integer. It corresponds to an MD5 authentication key contained in an authentication file (.txt) located on the server. This file must be on both the server and the local switch, and match, for authentication to work. Enter the key identification using the **key** keyword if the server is set to MD5 authentication.

- An authentication key is composed of a 32-bit integer and 32-byte string of characters. The integer format is hexadecimal. For an NTP message to be authenticated the NTP client authentication key must match the key configured at the NTP server. This means the authentication keys must be distributed in advance of configuring the NTP client. If authentication is disabled but authentication key is present, the association will still be unauthenticated.
- Use the **version** keyword to set the correct version of NTP.
- Use the **minpoll** keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds ($2^4 = 16$). The client will poll the server for a time update when the **minpoll** time is exceeded.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

ntp client Enables or disables NTP operation on the switch.

MIB Objects

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

ntp server synchronized

Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.

ntp server synchronized

Syntax Definitions

N/A

Defaults

By default, NTP synchronization is enabled.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

When NTP peer synchronization tests are disabled, the NTP client is able to synchronize with either an NTP peer that is not synchronized with an atomic clock or a network of NTP servers that will finally synchronize with an atomic clock.

Examples

```
-> ntp server unsynchronized
```

Release History

Release 7.1.1; 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 time synchronization discipline.

ntp client admin-state {enable | disable}

Syntax Definitions

enable	Enables NTP.
disable	Disables NTP.

Defaults

NTP protocol is disabled by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to enable or disable NTP. Before NTP can be enabled, an NTP server must be specified using the [ntp server](#) command. Up to 3 NTP servers may be defined.
- It is not necessary to specify an NTP server if the NTP client will only receive time updates from NTP broadcast servers.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

[ntp server](#) Specifies an NTP server from which the switch will receive updates.

MIB Objects

alaNtpEnable

ntp src-ip preferred

Configures a source IP address to use as the source for NTP packets.

```
ntp src-ip preferred {default | no-loopback0 | ip_address}
```

```
no ntp src-ip preferred
```

Syntax Definitions

default	The Loopback0 address, if configured, will be used for the source IP address field. If no Loopback0 is configured, the preferred IP address will be used. If no preferred IP address is configured the first available IP address on the switch will be used.
no-loopback0	The Loopback0 address will not be used for the source IP address field and either the preferred IP address (if configured) or the first available IP address on the switch will be used.
<i>ip_address</i>	The IP address to be used in the source IP field.

Defaults

By default, the NTP source ip preferred setting is set to the **default** parameter.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- By default The Loopback0 address, if configured, will be used for the source IP address field.
- If no Loopback0 is configured, the preferred IP address configured by the user will be used
- If no Loopback0 or preferred IP address is configured the first available IP address on the switch will be used.
- When configuring a preferred IP address, that address must already exist on the switch.
- Use the **no** form of this command to clear a specific IP address and change the behavior back to default.

Examples

```
-> ntp src-ip preferred 192.168.10.1  
-> ntp src-ip preferred no-loopback0  
-> ntp src-ip preferred default
```

Release History

Release 7.1.1; command was introduced

Related Commands**show ntp status**

Displays the NTP configuration and status.

MIB ObjectsN/A

ntp broadcast-client

Enables or disables the NTP client to receive time updates from NTP broadcast servers.

ntp broadcast-client {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 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

alaNtpBroadcastEnable

ntp broadcast-delay

Sets the broadcast delay time in microseconds of received NTP broadcast messages.

ntp broadcast-delay *microseconds*

Syntax Definitions

microseconds The number of microseconds for the broadcast delay.

Defaults

parameter	default
<i>microseconds</i>	4000

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; 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

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

Defaults

By default, all authentication key are untrusted.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Authentication keys are stored in a key file and loaded into memory when the switch boots. The keys loaded into memory are not trusted until this command is used. The location of the file containing set of generated authentication keys is /flash/network/ntp.keys.
- Once the keys are loaded into software (on boot up of the switch), they must be activated by being labeled as trusted. A trusted key will authenticate with a server that requires authentication as long as the key matches the server key.
- New keys must be added manually to the key file. A newly added key will not be loaded into the switch software until the **ntp key load** command is issued, or the switch is rebooted.
- An authentication key is composed of a 32-bit integer and 32-byte string of characters. The integer format is hexadecimal. For an NTP message to be authenticated the NTP client authentication key must match the key configured at the NTP server. This means the authentication keys must be distributed in advance of configuring the NTP client. If authentication is disabled but authentication key is present, the association will still be unauthenticated.
- By default all keys read from the ntp.conf key file are untrusted therefore keys must be set to 'trusted' status to allow NTP to use the key for authentication.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

```
alaNtpAccessKeyIdTable  
  alaNtpAccessKeyIdKeyId  
  alaNtpAccessKeyIdTrust
```

ntp key load

Loads the current key file into memory.

ntp key load

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command reloads the key file into the switch memory. This allows for new keys in the key file to be added to the list of keys the switch can use for authentication.
- Newly added keys must be labeled as **trusted** with the **ntp key** command before being used for authentication.
- By default, all authentication keys are untrusted therefore reloading a key file will change any current trusted keys to untrusted status.
- The file ntp.keys is used during the establishment of a set of authentication keys that are used by the NTP protocol. The location of this file is fixed in directory /flash/network.

Examples

```
-> ntp key load
```

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

alaNtpAccessRereadkeyFile

ntp authenticate

Enables or disables the authentication on a configured NTP server.

ntp authenticate {enable | disable}

Syntax Definitions

enable	Enables authentication for NTP server.
disable	Disables authentication for NTP server.

Defaults

By default, NTP authentication is disabled.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to enable or disable authentication for NTP server.
- Before NTP authentication is enabled, NTP operation should be enabled by using [ntp client](#) command.
- Before enabling the NTP operation, NTP server must be specified using the [ntp server](#) command.

Examples

```
-> ntp authenticate enable  
-> ntp authenticate disable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ntp status](#) Displays the information about the current NTP status.

MIB Objects

alaNtpAuthenticate

ntp master

Specifies the stratum value for unsynchronized switch to act as an authoritative NTP source.

ntp master *{stratum-number}*

Syntax Definitions

stratum-number Integer value ranging from 2 to 16

Defaults

Parameter	Default
<i>stratum-number</i>	16

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to synchronize improved clocks with lower strata value if any of the trustworthy NTP sources comes up.
- Use default value of 16 if switch is not synchronized with itself.
- When the switch is synchronized, the stratum number should correspond to peer/server.

Examples

```
-> ntp master 4
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ntp status](#) Displays current NTP status.

MIB Objects

alaNtpConfig
alaNtpSysStratum

ntp interface

Enables or Disables NTP server functionality for an interface.

ntp interface {*interface-ip*} {**enable** | **disable**}

Syntax Definitions

<i>interface-ip</i>	IP address of an interface on which NTP server functionality is to be disabled.
enable	Enables NTP server functionality on an interface.
disable	Disables NTP sever functionality on an interface.

Defaults

By default, NTP server functionality is enabled on all the interfaces.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to enable or disable the incoming NTP request.
- Disabling the NTP server functionality drops the NTP request on an interface and synchronization information is not sent out.

Examples

```
-> ntp interface 10.10.10.1 disable  
-> ntp interface 10.10.10.1 enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ntp status](#) Displays current NTP status.

MIB Objects

alaNtpAccessRestrictedTable
alaNtpAccessRestrictedIpAddress

ntp max-associations

Configures the maximum number of associations on the switch.

ntp max-associations *{number}*

Syntax Definitions

number Maximum no of client/server and peer associations. Integer value ranging from 0 to 64.

Defaults

By default, 32 associations are allowed on the switch.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to restrict the number of client/server and peer association.
- The command can be used to change the default value of 32 to any value between 0 to 64.
- The command protects the switch from overwhelming with the NTP requests. When the limit is reached, trap is sent to indicate the switch.

Examples

```
-> ntp max-associations 20
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ntp status](#) Displays current NTP status.

MIB Objects

alaNtpConfig
alaNtpMaxAssociation

ntp broadcast

Enables NTP to broadcast synchronized information to all the clients in the subnet in the configured interval.

ntp broadcast {*broadcast-addr*} [**version** *version*] [**minpoll** *poll interval*]

no ntp broadcast {*broadcast-addr*}

Syntax Definitions

<i>broadcast-addr</i>	Subnet for which broadcast updates are regularly sent.
<i>version</i>	NTP version on which the broadcast updates are sent out on the subnet for the clients. Value is 3 or 4.
<i>poll interval</i>	Polling interval for NTP broadcast message. This value is measured in seconds.

Defaults

Parameter	Default
<i>version</i>	4
<i>poll interval</i>	6

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to configure NTP to act in broadcast server mode.
- Use the **no** form of this command to remove the configured broadcast servers. This also disables NTP synchronization information being sent for that broadcast subset.
- The NTP broadcast address needs to be defined to enable NTP broadcast mode. A maximum of 3 broadcast addresses can be configured.
- Use the **version** keyword to set the correct version of NTP.
- Use the **minpoll** keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered.

Examples

```
-> ntp broadcast 10.145.59.255 version 4 minpoll 5
-> no ntp broadcast 10.145.59.255
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[ntp broadcast](#)

Enables or disables the client's broadcast mode.

[ntp broadcast-delay](#)

Sets the broadcast delay time in microseconds

MIB Objects

alaNtpPeerTable

 alaNtpPeerType

 alaNtpPeerVersion

 alaNtpPeerMinpoll

ntp peer

Configures NTP to operate in the symmetric active peering mode. This also enables the establishment of an active symmetric association with the specified remote peer.

ntp peer {*ip-address*} [**key** *keyid*] [**version** *version*] [**minpoll** *poll interval*]

no ntp peer {*ip-address*}

Syntax Definitions

<i>ip-address</i>	IP address of the remote peer.
<i>key-id</i>	Authentication key for the remote peer.
<i>version</i>	NTP packet version to be used for the peer association.
<i>poll interval</i>	Polling interval for NTP broadcast message. Poll interval which when expires, packets will be sent to the peer.

Defaults

Parameter	Default
<i>version</i>	4
<i>poll interval</i>	6

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use **no** form of this command to remove the peers that are configured to act in symmetric active mode. This command deletes the symmetric active association with the remote peer.
- Use the **version** keyword to set the correct version of NTP.
- Use the **minpoll** keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered.
- The command should not be used for b(Broadcast), m(Multicast) or r(Reference clock address 127.127.x.x)
- *ip-address* is the mandatory parameter to be entered in the command while key id is the optional parameter. If key id is not specified, then peering will not be authenticated.

Examples

```
-> ntp peer 172.18.16.112
-> no ntp peer 172.18.16.112
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show ntp peers](#) Displays current NTP peer association.

MIB Objects

```
alaNtpPeerTable  
  alaNtpPeerType  
  alaNtpPeerAuth  
  alaNtpPeerVersion  
  alaNtpPeerMinpoll
```

ntp vrf-name

Sets the VRF to be used for all NTP operations (both client and server).

ntp vrf-name *name*

Syntax Definitions

name The name of the VRF to be used for all NTP operations.

Defaults

Parameter	Default
<i>name</i>	default

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ntp vrf-name vrf1
```

Release History

Release 7.3.1; command introduced.

Related Commands

[show ntp status](#) Displays the information about the current NTP status.
[show ntp client](#) Displays information about the current client NTP configuration.

MIB Objects

alaIpNtpVrfName

show ntp status

Displays the information about the current NTP status.

show ntp status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command displays the information about the status of NTP, which is configured along with other global configuration. See the Examples section for more information.
- If the source IP Configuration is done in default or no-loopback0 then the source ip-address will not be displayed in the output of the **show ntp status** command.

Example

```
-> show ntp status
Current time:                Thu, Jun 14 2012 21:05:46.313 (UTC),
Last NTP update:            -,
Server reference:           0.0.0.0,
Client mode:                 disabled,
Broadcast client mode:      disabled,
Broadcast delay (microseconds): 4000,
Server qualification:       synchronized,
Stratum:                     16,
Maximum Associations Allowed: 32,
Authentication:             disabled,
Source IP Configuration:    default
VRF Name:                   default
```

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	The source of the time signal, which is the address of the NTP server that provided the currently-used time update.
Client mode	Whether the NTP client software is enabled or disabled.
Broadcast client mode	What NTP mode the client is running in, either client or broadcast.
Broadcast delay	The number of microseconds in the advertised broadcast delay time. This field is absent if the client broadcast mode is disabled.
Server qualification	Server qualification status.
Stratum	The stratum of the server. The stratum number is the number of hops from a UTC time source.
Max-Association	Maximum association on the switch that restricts the number of client/server and peer association
Authentication	Whether Authentication is enabled or disabled
Source IP Configuration	Source IP Configuration type which is configured.
Source IP	Source IP address for NTP that send updates to clients. Note: This field is displayed only if the value of "Source IP Configuration" is set to "Preferred".
VRF Name	Name of the VRF.

Release History

Release 7.1.1; command introduced.
Release 7.3.1; **vrf** parameter added.

Related Command

ntp client	Enables or disables NTP operation on the switch.
ntp server	Specifies an NTP server from which the switch will receive updates
ntp server synchronized	Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.
ntp max-associations	Configures the maximum number of associations on the switch.
ntp master	Specifies the stratum value for unsynchronized switch
ntp broadcast	Enables or disables the client's broadcast mode.
show ntp client	Displays information about the current client NTP configuration.
show ntp client server-list	Displays a list of the servers with which the NTP client synchronizes
show ntp server client-list	Displays the basic server information for a specific NTP server or a list of NTP servers

MIB Objects

```
alaNtpPeerListTable  
  alaNtpPeerShowOriginateTime  
  alaNtpPeerShowTransmitTime  
  alaNtpEnable  
  alaNtpBroadcastEnable  
  alaNtpBroadcastDelay  
  alaNtpPeerTests  
  alaNtpPeerStratum  
  alaNtpPeerTests  
  alaNtpAuthenticate  
  alaNtpSrcIpConfig  
  alaNtpSrcTp  
  alaIpNtpVrfName
```

show ntp client

Displays information about the current client NTP configuration.

show ntp client

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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:                Tue, Jun 26 2012 17:52:47.619 (UTC),
Last NTP update:            (null),
Server reference:           0.0.0.0,
Client mode:                 disabled,
Broadcast client mode:      disabled,
Broadcast delay (microseconds): 4000,
Server qualification:       synchronized
VRF Name:                   default
```

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	The source of the time signal, which is the address of the NTP server that provided the currently-used time update.
Client mode	Whether the NTP client software is enabled or disabled.
Broadcast client mode	What NTP mode the client is running in, either client or broadcast.
Broadcast delay	The number of microseconds in the advertised broadcast delay time. This field is absent if the client broadcast mode is disabled.
Server Qualification	Indicates whether the server must be synchronized or not.
VRF Name	Name of the VRF.

Release History

Release 7.1.1; command was introduced.

Related Command

ntp client

Enables or disables NTP operation on the switch.

MIB Objects

alaNtpLocalInfo
alaIpNtpVrfName

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 10K, 6900

Usage Guidelines

Use this command to display tabular information on the current NTP client to server association status.

Examples

```
-> show ntp client server-list
IP Address      Ver  Key  St   Delay      Offset      Disp
=====+====+=====+====+=====+=====+=====
*198.206.181.70  4    0   2    0.167      0.323      0.016
=198.206.181.123 4    0  16    0.000      0.000      0.000
```

output definitions

IP Address	The server IP address. "+" indicates an active peer "-" indicates a pasive peer "=" indicates a client "*" indicates current system peer "^" indicates a broadcast server "\" indicates a broadcast client
Ver	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server, or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.
St	The stratum of the server.
Delay	The delay received from the server in its timestamp.
Offset	The offset received from the server in its timestamp.
Disp	The dispersion value received from the server in its timestamp.

Release History

Release 7.1.1; command was introduced.

Related Command

ntp client

Enables or disables NTP operation on the switch.

MIB Objects

alaNtpPeerListTable

show ntp server client-list

Displays the information about the current NTP clients connected to the server.

show ntp server client-list

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use this command to display the tabular information on the current NTP client connected to the server (switch).

Examples

```
-> show ntp server client-list
IP Address          Ver      Key
-----+-----+-----
172.23.0.201        4         0
10.255.24.121       4         0
```

output definitions

IP Address	The client IP address.
Ver	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.

Release History

Release 7.1.1; command was introduced.

Related Command**show ntp status**

Displays information about the current client NTP configuration

ntp client

Enables or disables NTP operation on the switch.

MIB Objects

```
alaNtpClientListTable  
  alaNtpPeerListAddress  
  alaNtpPeerVersion  
  alaNtpPeerAuth
```

show ntp server status

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

show ntp server status [*ip_address*]

Syntax Definitions

ip_address The IP address of the NTP server to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command displays information on the status of any or all configured NTP servers/peers.
- To display a specific server, enter the command with the server's IP address. To display all servers, enter the command with no server IP address.

Examples

```
-> show ntp server status
IP address      = 172.18.16.147,
Host mode      = server,
Peer mode      = unspec,
Prefer         = no,
Version        = 4,
Key            = 0,
Stratum        = 16,
Minpoll        = 4 (16 seconds),
Maxpoll        = 10 (1024 seconds),
Delay          = 0.000 seconds,
Offset         = 0.000 seconds,
Dispersion     = 0.000 seconds
Root distance  = 0.000,
Precision      = -6,
Reference IP   = 0.0.0.0,
Status         = not configured,
Uptime count   = 28250 seconds,
Reachability   = 0,
Unreachable count = 5,
Stats reset count = 27829 seconds,
Packets sent   = 0,
Packets received = 0,
Duplicate packets = 0,
Bogus origin   = 0,
Bad authentication = 0,
Bad dispersion  = 0
```

```
IP address      = 172.18.16.147,
Host mode       = server,
Peer mode       = unspec,
Prefer          = no,
Version         = 4,
Key             = 0,
Stratum         = 16,
Minpoll         = 4 (16 seconds),
Maxpoll         = 10 (1024 seconds),
Delay           = 0.000 seconds,
Offset          = 0.000 seconds,
Dispersion      = 0.000 seconds
Root distance   = 0.000,
Precision       = -6,
Reference IP    = 0.0.0.0,
Status          = not configured,
Uptime count    = 28250 seconds,
Reachability    = 0,
Unreachable count = 16,
Stats reset count = 26812 seconds,
Packets sent    = 0,
Packets received = 0,
Duplicate packets = 0,
Bogus origin    = 0,
Bad authentication = 0,
Bad dispersion  = 0

-> show ntp server status 198.206.181.139
IP address      = 198.206.181.139,
Host mode       = client,
Peer mode       = server,
Prefer          = no,
Version         = 4,
Key             = 0,
Stratum         = 2,
Minpoll         = 6 (64 seconds),
Maxpoll         = 10 (1024 seconds),
Delay           = 0.016 seconds,
Offset          = -180.232 seconds,
Dispersion      = 7.945 seconds
Root distance   = 0.026,
Precision       = -14,
Reference IP    = 209.81.9.7,
Status          = configured : reachable : rejected,
Uptime count    = 1742 seconds,
Reachability    = 1,
Unreachable count = 0,
Stats reset count = 1680 seconds,
Packets sent    = 1,
Packets received = 1,
Duplicate packets = 0,
Bogus origin    = 0,
Bad authentication = 0,
Bad dispersion  = 0,
Last Event      = peer changed to reachable,
```

output definitions

IP address	The server IP address.
Host mode	The host mode of this remote association.
Peer mode	The peer mode of this remote association.
Prefer	Whether this server is a preferred server or not. A preferred server is used to synchronize the client before a non-preferred server.
Version	The version of NTP the server is using. Versions 3 and 4 are valid.
Key	The NTP server's public key. This must be accurate and the same as the NTP server, or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.
Stratum	The stratum of the server. The stratum number is the number of hops from a UTC time source.
Minpoll	The minimum poll time. The client will poll the server for a time update every time this limit has been exceeded.
Maxpoll	The maximum poll time.
Delay	The delay received from the server in its timestamp.
Offset	The offset received from the server in its timestamp.
Dispersion	The dispersion value received from the server in its timestamp.
Root distance	The total round trip delay (in seconds) to the primary reference source.
Precision	The advertised precision of this association.
Reference IP	The IP address identifying the peer's primary reference source.
Status	The peer selection and association status.
Uptime count	The time period (in seconds) during which the local NTP server was associated with the switch.
Reachability	The reachability status of the peer.
Unreachable count	Number of times the NTP entity was unreachable.
Stats reset count	The time delay (in seconds) since the last time the local NTP server was restarted.
Packets sent	Number of packets sent.
Packets received	Number of packets received.
Duplicate packets	Number of duplicated packets received.
Bogus origin	Number of bogus packets.
Bad authentication	Number of NTP packets rejected for not meeting the authentication standards.
Bad dispersion	Number of bad dispersions.
Last Event	The last event.

Release History

Release 7.1.1; command was introduced.

Related Command**ntp client**

Enables or disables NTP operation on the switch.

MIB Objects

alaNtpPeerListTable

 alaNtpPeerShowStatus

show ntp keys

Displays information about all authentication keys.

show ntp keys

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays the information on the current set of trusted authentication keys.

Examples

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

output definitions

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

Release History

Release 7.1.1; command was introduced.

Related Command

ntp key Labels the specified authentication key identification as trusted or untrusted.

ntp key load Loads the current key file into memory.

MIB Objects

alaNtpAccessKeyIdTable

show ntp peers

Displays the information about the current status on the NTP peer association.

show ntp peers

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Use this command to display the tabular information on the current NTP peer association status.

Examples

```
-> show ntp peers
IP Address      Ver    Key    St    Delay    Offset    Disp
-----+-----+-----+-----+-----+-----+-----
172.23.0.202    4      0     3     0.300    0.404    0.0024
10.255.24.120   4      0     3     0.016    0.250    0.0017
```

output definitions

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

Release History

Release 7.1.1; command was introduced.

Related Command**ntp client**

Enables or disables NTP operation on the switch.

show ntp status

Displays the information about the current NTP status.

show ntp server status

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

MIB Objects

```
alaNtpPeerListTable  
  alaNtpPeerListAddress  
  alaNtpPeerVersion  
  alaNtpPeerAuth  
  alaNtpPeerStratum  
  alaNtpPeerListDelay  
  alaNtpPeerShowOffset  
  alaNtpPeerListDispersion
```

show ntp server disabled-interfaces

Displays the ip addresses of the interfaces on which NTP server is not enabled.

show ntp server disabled-interfaces

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

This command displays ip interfaces on which currently NTP server functionality is disabled.

Examples

```
-> show ntp server disabled-interfaces
IP Address
-----
172.23.0.202
10.255.24.120
```

output definitions

IP Address	Peer IP Address
------------	-----------------

Release History

Release 7.1.1; command was introduced.

Related Command

[show ntp status](#)

Displays the information about the current NTP status.

[show ntp server status](#)

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

MIB Objects

alaNtpAccessRestrictedTable
alaNtpPeerListAddress

49 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:

	OmniSwitch 10K
Telnet(v4)	4
FTP(v4)	4
SSH + SFTP(v4)	8
HTTP	4

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**
- session xon-xoff**
- show prefix**
- user profile save**
- user profile reset**
- history**
- command-log**
- kill**
- exit**
- who**
- whoami**
- show session config**
- show session xon-xoff**
- more**
- telnet**
- ssh**
- ssh enforce-pubkey-auth**
- show command-log status**
- show telnet**
- show ssh**

session login-attempt

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

session login-attempt *integer*

Syntax Definitions

integer

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

Defaults

Default is 3 login attempts.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

[show session config](#)

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

[session login-timeout](#)

Sets or resets the amount of time the user can take to accomplish a successful login to the switch.

[session timeout](#)

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

MIB Objects

sessionMgr

sessionLoginAttempt

session login-timeout

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

session login-timeout *seconds*

Syntax Definitions

seconds

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

Defaults

Login timeout default is 55 seconds.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

[show session config](#)

Displays Session Manager information such as banner file name, session timeout value, default prompt value, login timer, and login attempt number.

[session login-attempt](#)

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

[session timeout](#)

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

MIB Objects

sessionMgr

sessionLoginTimeout

session banner

Sets or resets the file name of the user-defined banner. The banner is a welcome banner that appears after the user successfully logs onto the switch.

```
session {cli | ftp | http} banner file_name
```

```
no session {cli | ftp | http} banner
```

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.
<i>file_name</i>	Banner file name including the path from the switch's /flash directory. The maximum length of the filename and path is 255 characters.

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The **no session banner** command is used to disable a user defined session banner file from displaying when you log onto the switch.
- The **session banner** command is used to configure or modify the banner file *name*. You must use a text editor to edit the file containing the banner text.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

[show session config](#)

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

MIB Objects

SessionConfigTable

 SessionType

 SessionBannerFileName

session timeout

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

```
session {cli | http | ftp} timeout 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.
<i>minutes</i>	Inactivity timeout value (in minutes). Valid range 1 to 596523.

Defaults

parameter	default
<i>minutes</i>	4

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The inactivity timer value may 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 cli timeout 5
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show session config](#)

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

MIB Objects

SessionConfigTable

 SessionType

 SessionInactivityTimerValue

session prompt

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

session prompt default [*string*]

Syntax Definitions

string Prompt string. Maximum length 31 characters.

Defaults

parameter	default
<i>string</i>	->

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The new prompt will not take effect until you log off and back onto the switch.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

[show session config](#) Displays Session Manager information such as banner file name, session timeout value, and default prompt value.

MIB Objects

SessionConfigTable
 SessionType
 sessionDefaultPromptString

session xon-xoff

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

session xon-xoff {enable | disable}

Syntax Definitions

enable Enables XON-XOFF on the console port.

disable Disables XON-XOFF on the console port.

Defaults

parameter	default
enable / disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

sessionXonXoffEnable

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 10K, 6900

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 7.1.1; command was introduced.

Related Commands

[show prefix](#)

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

MIB Objects

N/A

user profile save

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

user profile save

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to save prompt definitions and more mode screen settings for use in future login sessions for the current user account.
- Use the **user profile reset** command to set values to their factory defaults.

Examples

```
-> user profile save
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|------------------------------------|--|
| show prefix | Defines substitute command text for the switch's CLI command keywords. |
| 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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> user profile reset
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[show prefix](#)

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

[user profile save](#)

Saves the user account settings for aliases, prompts and the more screen.

MIB Objects

N/A

history

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

history *number*

Syntax Definitions

number The number of commands to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> history
1 show cmm
2 show fan
3 show sensor
```

output definitions

Index	The index of the commands for this CLI session and the associated command.
--------------	--

Release History

Release 7.1.1; command was introduced.

Related Commands

! 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 10K, 6900

Usage Guidelines

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

Examples

```
-> history
1* show ip interface
2 show vlan
3 show arp
4 clear arp
->!2
show vlan
vlan  type  admin  oper  ip    mtu   name
-----+-----+-----+-----+-----+-----+-----
   1   std    Ena    Ena   Dis   1500  VLAN 1
  10   std    Ena    Ena   Ena   1500  VLAN 10
  12   std    Ena    Ena   Ena   1500  VLAN 12
  14   std    Ena    Ena   Ena   1500  VLAN 14
  30   vip    Ena    Ena   Ena   1500  VIP VLAN 30
  40   vip    Ena    Ena   Ena   1500  VIP VLAN 40
4094  mcm    Ena    Ena   Dis   9198  MCM IPC
```

Release History

Release 7.1.1; command was introduced.

Related Commands**history**

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

MIB Objects

N/A

command-log

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

command-log {enable | disable}

Syntax Definitions

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

Defaults

parameter	default
enable disable	disable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

sessionCliCommandLogEnable

kill

Kills an active session. The command takes effect immediately.

kill *session_number*

Syntax Definitions

session_number Number of the session you want to kill.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

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

MIB Objects

SessionMgr
 sessionIndex
 sessionRowStatus

exit

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

exit

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> exit
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[kill](#) Kills an active session. The command takes effect immediately.

MIB Objects

```
SessionMgr  
  sessionIndex  
  sessionRowStatus
```

whoami

Displays the current user session.

whoami

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 = ,
```

output definitions

Session Number	The session number assigned to the user.
User name	User name.
Access type	Type of access protocol used to connect to the switch.
Access port	Switch port used for access during this session.
Ip Address	User IP address.
Read-only domains	The command domains available with the user's read-only access.
Read-only families	The command families available with the user's read-only access.
Read-Write domains	The command domains available with the user's read-write access.
Read-Write families	The command families available with the user's read-write access.

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

SessionActive

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

who

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

who

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

You can identify your current login session by using IP address.

Examples

```

-> who
Session number = 0
  User name   = (at login),
  Access type = console,
  Access port = Local,
  IP address  = 0.0.0.0,
  Read-only domains = None,
  Read-only families = ,
  Read-Write domains = None,
  Read-Write families = ,

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 = ,

```

output definitions

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

output definitions (continued)

Ip Address	User IP address.
Read-only domains	The command domains available with the user's read-only access.
Read-only families	The command families available with the user's read-only access.
Read-Write domains	The command domains available with the user's read-write access.
Read-Write families	The command families available with the user's read-write access.

Possible values for command domains and families are listed here:

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

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

show session config

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

show session config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

```
-> show session config
```

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

output definitions

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

output definitions (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 into the switch before the TCP connection is closed.

Release History

Release 7.1.1; command was introduced.

Related Commands

session prompt	Configures the default CLI prompt for console and Telnet sessions.
session banner	Sets the file name of the user-defined banner.
session timeout	Configures the inactivity timer for a CLI, HTTP (including Web-View), or FTP interface.
session login-attempt	Sets the number of times a user can attempt to log into 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 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

[session xon-xoff](#) Enables/disables the XON-XOFF protocol on the console port.

MIB Objects

```
sessionXonXoffEnable
```

more

Enables the more mode for your console screen display.

more *filename*

Syntax Definitions

filename The file to display.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This parametr can also be used to pipe output from the CLI.
- This command is case sensitive.

Examples

```
-> more textfile.txt  
-> write terminal | more
```

Release History

Release 7.1.1; command was introduced.

Related Commands

MIB Objects

```
SystemServices  
  systemServicesArg1  
  systemServicesAction
```

telnet

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

```
[vrf name] telnet {port [default | service_port] | admin-state [enable | disable] | host_name | ip_address}
```

Syntax Definitions

<i>name</i>	Name of the VRF.
default	Sets the port back to the default of 23.
<i>service_port</i>	The TCP service port number. Must be 23 or between 20000-20999.
enable disable	Enables or disables telnet access.
<i>host_name</i>	Specifies the host name for the Telnet session.
<i>ip_address</i>	Specifies the IPv4 or IPv6 address for the Telnet session.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The default directory for Telnet is **/flash**.

Examples

```
-> telnet port 20999
-> telnet admin-state disable
-> telnet 172.17.6.228
-> vrf vrf1 telnet admin-state enable
```

Release History

Release 7.1.1; command introduced.

Related Commands

ssh	Invokes the Secure Shell on the switch. A Secure Shell is used to make a secured connection to a remote system or device.
show telnet	Displays the current configuration specifying the ports the telnet daemons are listening on.

MIB Objects

SystemServices

- systemServicesArg1
- systemServicesAction
- alaIpTelnetAdminStatus

ssh

Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.

```
[vrf name] ssh {port [default | service_port] | admin-state [enable | disable] | host_name | ip_address}
```

Syntax Definitions

<i>name</i>	Name of the VRF.
default	Sets the port back to the default of 23.
<i>service_port</i>	The TCP service port number. Must be 23 or between 20000-20999.
enable disable	Enables or disables telnet access.
<i>host_name</i>	Specifies the host name for Secure Shell.
<i>ip_address</i>	Specifies the IPv4 or IPv6 address for Secure Shell.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

```
-> ssh port 20000
-> ssh admin-state disable
-> ssh 172.155.11.211
login as:

-> vrf vrf1 ssh admin-state enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

telnet	Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.
ssh enforce-pubkey-auth	Invokes Secure Shellv6 on the switch. Secure Shellv6 is used to make a secured connection to an SSHv6 server.
show command-log	Displays the status of Secure Shell, SCP/SFTP on the switch.
show ssh	Displays the current configuration specifying the ports SSH daemons are listening on.

MIB Objects

```
aaaAcctSatable
  aaacsInterface
alaSshConfigGroup
  alaIpSshAdminStatus
```

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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> ssh enforce-pubkey-auth enable
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[telnet](#) Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.

MIB Objects

alaSshConfigGroup
 alaSshPubKeyEnforceAdminStatus

show command-log

Displays the contents of the **command.log** file. This file contains a record of all CLI commands executed on the switch since the command logging function was enabled. For more information on enabling and disabling command logging, refer to [page 49-17](#).

show command-log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The most recent commands are listed first.
- The command history is archived to the **command.log** file. If this file is removed, the command history will no longer be available. In addition, the **command.log** file has a 66,402 byte capacity. This capacity allows up to 100 commands; if the maximum capacity is reached, only the 100 most recent commands display.

Examples

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

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

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

output definitions

Command	The exact syntax of the command, as entered by the user.
UserName	The name of the user session that entered the command. For more information on different user session names, refer to the user command on page 31-21 , or the “Managing Switch User Accounts” chapter in the <i>Switch Management Guide</i> .
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 7.1.1; command was introduced.

Related Commands

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

MIB Objects

sessionCliCommandLogEnable

show command-log status

Shows the current status of the command logging function (i.e., enabled or disabled).

show command-log status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

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

output definitions

CLI command logging	The current status of command logging on the switch. Options include Disable and Enable .
----------------------------	---

Release History

Release 7.1.1; command was introduced.

Related Commands

[command-log](#) Enables or disables command logging on the switch.

MIB Objects

sessionCliCommandLogStatus

show telnet

Displays the current configuration specifying the ports the telnet daemons are listening on.

[vrf name] show telnet

Syntax Definitions

name Name of the VRF.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

If VRF is specified, the current status of the telnet daemon for the speciifed VRF is displayed.

Examples

```
vrf1::-> show telnet
Telnet Admin-State = Enabled
Telnet Port = 23
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[command-log](#) Enables or disables command logging on the switch.

MIB Objects

```
alaIpTelnetAdminStatus
alaIpTelnetPort
```

50 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 memory usage on the switch.

MIB information for the system commands is listed here:

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 rm cp scp mv chmod freespace fsck newfs rcp rrm rls
System Services	vi tty show tty tftp sftp ftp show ftp

cd

Changes the current working directory of the switch.

cd [*path*]

Syntax Definitions

path

Specifies the path to the working directory. If no path is specified, the current directory of the switch is changed to the higher directory level.

Defaults

The default working directory of the switch is **/flash**.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Separate the multiple directory names that are part of the path with a slash (/).

Examples

```
-> cd
-> cd /flash/certified
```

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

```
systemServices
  systemServicesWorkingDirectory
```

pwd

Displays the current working directory of the switch.

pwd

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The **pwd** command can also be used on the secondary CMM.

Examples

```
-> pwd  
/flash
```

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

```
systemServices  
  systemServicesWorkingDirectory
```

mkdir

Creates a new directory.

mkdir [*options*] [*path*] /*dirname*

Syntax Definitions

<i>options</i>	Use the '?' on the command line for a list of options.
<i>path</i>	The path or location in which the new directory is to be created. If no path name is specified, the new directory is created in the current directory.
<i>dirname</i>	A user-defined name for the new directory.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Separate the directory names that are part of the path with a slash (/). Refer to the examples below.
- The **mkdir** command can also be used on the secondary CMM.

Examples

```
-> mkdir test_directory
-> mkdir flash/test_directory
-> mkdir
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.
```

```
Usage: mkdir [OPTIONS] DIRECTORY...
```

```
Create DIRECTORY
```

```
Options:
```

```
  -m      Mode
  -p      No error if exists; make parent directories as needed
```

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

```
systemServices
  systemServicesArg1
  systemServicesAction
```

rmdir

Deletes an existing directory.

rmdir [*options*] *dirname*

Syntax Definitions

options Use the '?' on the command line for a list of options.
dirname The name of the existing directory to be removed.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Separate the directory names that are part of the path with a slash (/). Refer to the examples below.
- This command can also be used on the secondary CMM.

Examples

```
-> rmdir ./working
-> rmdir flash/working
-> rmdir ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.
```

Usage: rmdir [OPTIONS] DIRECTORY...

Remove DIRECTORY if it is empty

Options:

```
-p|--parents        Include parents
--ignore-fail-on-non-empty
```

Release History

Release 7.1.1; command introduced.

Related Commands

cd	Changes the current working directory of the switch.
pwd	Displays the current working directory of the switch.
mkdir	Creates a new directory.
ls	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 [*options*] [*path/filename*]

Syntax Definitions

options Use the '?' on the command line for a list of options.
filename Specifies the file or directory path.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

Separate the multiple directory names that are part of the path with a slash (/).

Examples

```
-> ls
-> ls -l /flash/certified
-> ls ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.
```

```
Usage: ls [-lAacCddeFfiLlpRSrStuvwxXhk] [FILE]...
```

List directory contents

Options:

```
-l      List in a single column
-A      Don't list . and ..
-a      Don't hide entries starting with .
-C      List by columns
-c      With -l: sort by ctime
--color[={always,never,auto}] Control coloring
-d      List directory entries instead of contents
-e      List full date and time
-F      Append indicator (one of */=@|) to entries
-i      List inode numbers
-l      Long listing format
-n      List numeric UIDs and GIDs instead of names
-p      Append indicator (one of */=@|) to entries
-L      List entries pointed to by symlinks
-R      Recurse
-r      Sort in reverse order
-S      Sort by file size
-s      List the size of each file, in blocks
-T N    Assume tabstop every N columns
```

-t With -l: sort by modification time
-u With -l: sort by access time
-v Sort by version
-w N Assume the terminal is N columns wide
-x List by lines
-X Sort by extension
-h List sizes in human readable format (1K 243M 2G)

Release History

Release 7.1.1; command introduced.

Related Commands

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

MIB Objects

systemServices
 systemServicesArg1
 systemServicesAction

rm

Permanently deletes an existing file.

rm [*options*] [*path/filename*]

Syntax Definitions

<i>options</i>	Use the '?' on the command line for a list of options.
<i>filename</i>	Specifies the file or directory path.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Separate the multiple directory names that are part of the path with a slash (/). Refer to the examples below.
- Use care when deleting files. Depending on your switch and network configurations, specific configuration and image files must be present for your system to work properly.
- This command can also be used on the secondary CMM.

Examples

```
-> rm test_config_file
-> rm flash/test_config_file
-> rm ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.
```

```
Usage: rm [OPTIONS] FILE...
```

Remove (unlink) FILEs

Options:

-i	Always prompt before removing
-f	Never prompt
-R, -r	Recurse

Release History

Release 7.1.1; command introduced.

Related Commands**cp**

Copies 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 [options] source destination`

Syntax Definitions

<i>options</i>	Use the '?' on the command line for a list of options.
<i>source</i>	The name of the existing file to be copied.
<i>destination</i>	The new user-defined file name for the resulting file copy. If you are copying a file to the same directory as the original, the file name for the copy must be different from the original.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You should verify that the **/flash** directory of your switch has enough available memory to hold the copies of the files and directories created.
- A file can be copied to a new directory location. Copy of a file can also be created in the same directory that contains the original file.
- Separate the multiple directory names that are part of the path with a slash (/). Refer to the examples below.
- 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
```

```
-> cp ?
```

```
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.
```

Usage: cp [OPTIONS] SOURCE DEST

Copy SOURCE to DEST, or multiple SOURCE(s) to DIRECTORY

Options:

<code>-a</code>	Same as <code>-dpR</code>
<code>-R,-r</code>	Recurse
<code>-d,-P</code>	Preserve symlinks (default if <code>-R</code>)
<code>-L</code>	Follow all symlinks

```
-H      Follow symlinks on command line
-p      Preserve file attributes if possible
-f      Force overwrite
-i      Prompt before overwrite
-l, -s  Create (sym)links
```

Release History

Release 7.1.1; command 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 [options] user_name@remote_ip_addr:[path/]source [path/]target
```

```
scp [options] [path/]source user_name@remote_ip_addr:[path/]target
```

Syntax Definitions

<i>options</i>	Use the '?' on the command line for a list of options.
<i>user_name@remote_ip_addr:</i>	The username along with the IPv4 or IPv6 address of the remote switch.
<i>path/</i>	Specifies the path containing the file to be copied and the path where the file will be copied.
<i>source</i>	The name of the file(s) to be copied.
<i>target</i>	The new user-defined file name for the resulting file copy.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- This command will prompt you to enter the admin password, and the names and the path of the files being copied will be displayed.
- A file may be copied to a new location; you are not required to copy a file to the same directory that contains the original.
- Separate the multiple directory names that are part of the path with a slash (/). Refer to the examples below.

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.
```

```
-> scp ?
```

```
usage: scp [-1246BCpqr] [-c cipher] [-F ssh_config] [-i identity_file]
          [-l limit] [-o ssh_option] [-P port] [-S program]
          [[user@]host1:]file1 ... [[user@]host2:]file2
```

Release History

Release 7.1.1; command 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 [*options*] *source destination*

Syntax Definitions

<i>options</i>	Use the '?' on the command line for a list of options.
<i>source</i>	The name of the existing file to be copied.
<i>destination</i>	The new user-defined file name for the resulting file copy. If you are copying a file to the same directory as the original, the file name for the copy must be different from the original.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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.
- Separate the directory names and file names that are part of the path with a slash (/). Refer to the examples below.
- This command can also be used on the secondary CMM.

Examples

```
-> mv flash/asc.1.snap flash/backup_files/asc.1.snap
-> mv ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.
```

```
Usage: mv [OPTIONS] SOURCE DEST
or: mv [OPTIONS] SOURCE... DIRECTORY
```

Rename SOURCE to DEST, or move SOURCE(s) to DIRECTORY

Options:

```
-f      Don't prompt before overwriting
-i      Interactive, prompt before overwrite
```

Release History

Release 7.1.1; command introduced.

Related Commands

- rm** 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

<code>+w</code>	Enables read-write privileges for the file.
<code>-w</code>	Disables write privileges for the file—i.e., the file becomes read-only.
<code>path/</code>	The path containing the file for which privileges are being changed.
<code>file</code>	The name of the file for which read-write privileges are being changed.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

[freespace](#) 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** | **/uflash**]

Syntax Definitions

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

/uflash The amount of free space is shown for the **/uflash** directory.

Defaults

N/A

Usage Guidelines

N/A

Platforms Supported

OmniSwitch 10K, 6900

Examples

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

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

Release History

Release 7.1.1; command 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 /uflash {repair | no-repair}

Syntax Definitions

/uflash	Indicates that the file system check will be performed on the /uflash directory.
repair	Attempt to repair any problems found.
no-repair	Do not attempt to repair any problems found.

Defaults

This command gives you the option of having the errors repaired automatically.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- N/A

Examples

```
-> fsck /uflash repair
```

```
/uflash/ - disk check in progress ..  
/uflash/ - Volume is OK  
  
total # of clusters: 14,773  
# of free clusters: 4,132  
# of bad clusters: 0  
total free space: 8,264 Kb  
max contiguous free space: 5,163,008 bytes  
# of files: 46  
# of folders: 3  
total bytes in files: 21,229 Kb  
# of lost chains: 0  
total bytes in lost chains: 0
```

Release History

Release 7.1.1; command introduced.

Related Commands

freespace

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

MIB Objects

systemServices

 systemServicesArg1

 systemServicesAction

newfs

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

newfs /uflash

Syntax Definitions

/uflash This indicates that the complete file system will be replaced.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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.

Examples

```
-> newfs /uflash
```

Release History

Release 7.1.1; command introduced.

Related Commands

N/A

MIB Objects

```
systemServices  
  systemServicesArg1  
  systemServicesAction
```

rcp

Copies a file from a primary to a secondary CMM and vice versa.

rcp [**rem-slot:** *source_filepath destination_filepath*]

Syntax Definitions

<i>slot</i>	The slot number of the non-primary switch in a stack.
<i>source_filepath</i>	The name and path of the source file.
<i>destination_filepath</i>	The name and path of the destination file.

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

- This command can be used to copy files between CMMs.

Examples

```
-> rcp cmm-b:/flash/file.txt file.txt
```

```
-> rcp /flash/working/file.txt cmm-b:/flash/working/file.txt
```

Release History

Release 7.1.1; command introduced.

Related Commands

rrm	Removes a file from a secondary CMM.
rls	Displays the contents of a secondary CMM.

MIB Objects

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

rls

Displays the contents of the secondary CMM.

rls *directory* [*file_name*]

Syntax Definitions

directory The name of the directory on the non-primary CMM or switch.
file_name The file to be displayed on the non-primary CMM or switch.

Defaults

N/A

Platforms Supported

OmniSwitch 10K

Usage Guidelines

- Use this command to display the directory content on the secondary CMM.

Examples

```
-> rls /flash
drw      4096  Nov 11 10:00  ./
drw      0     Nov 11 09:55  ../
drw     16384  Nov 04 09:40  lost+found/
drw      4096  Nov 11 09:53  certified/
drw      4096  Nov 11 10:00  foss/
drw      4096  Nov 04 09:41  system/
-rw     70080  Nov 11 10:03  swlog
drw      4096  Nov 10 17:52  pmd/
drw      4096  Nov 11 10:01  switch/
drw      4096  Nov 04 09:41  network/
-rw     128071 Nov 11 10:00  swlog.0
drw      4096  Nov 11 10:00  working/
-rw     128016 Nov 11 09:53  swlog.1
-rw     128104 Nov 11 09:48  swlog.2
drw      4096  Nov 10 11:51  issu/
```

Release History

Release 7.1.1; command introduced.

Related Commands

rcp

Copies a file between CMMs.

rrm

Removes a file from a secondary CMM.

MIB Objects

chasSupervisionRfsLsTable

- chasSupervisionRfsLsFileIndex
- chasSupervisionRfsLsSlot
- chasSupervisionRfsLsDirName
- chasSupervisionRfsLsFileName
- chasSupervisionRfsLsFileType
- chasSupervisionRfsLsFileSize
- chasSupervisionRfsLsFileAttr
- chasSupervisionRfsLsFileDateTime

vi

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

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

Syntax Definitions

<i>options</i>	Use the '?' on the command line for a list of options.
<i>path</i>	The path (i.e., location) containing the file being viewed or edited. If no path is specified, the command assumes the current directory.
<i>filename</i>	The name of the existing file being viewed or edited.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

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

Examples

```
-> vi test_config_file
-> vi ?
BusyBox v1.16.1 (2010-12-06 23:23:38 PST) multi-call binary.
```

```
Usage: vi [OPTIONS] [FILE]...
```

```
Edit FILE
```

```
Options:
```

```
-c      Initial command to run ($EXINIT also available)
-R      Read-only
-H      Short help regarding available features
```

Release History

Release 7.1.1; command introduced.

Related Commands

vi

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
```

Related Commands

tty

Displays current TTY settings.

MIB Objects

```
systemServices
  systemServicesTtyLines
  systemServicesTtyColumns
```

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

<i>lines</i>	The number of lines to be displayed on the terminal emulation screen for the current session. Values may range from 10 to 150.
<i>columns</i>	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
<i>lines</i>	24
<i>columns</i>	80

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The number of lines and columns set with this command controls the screen size when the switch is editing or viewing a text file with the **vi** or **tftp** 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 7.1.1; command was introduced.

Related Commands

show tty Displays current TTY settings.

MIB Objects

```
systemServices
  systemServicesTtyLines
  systemServicesTtyColumns
```

show tty

Displays current TTY settings.

`show tty`

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command introduced.

Related Commands

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

MIB Objects

```
systemServices  
  systemServicesTtyLines  
  systemServicesTtyColumns
```

tftp

Starts a TFTP client session that enables a file transfer to an TFTP server.

tftp [*options*] *host* [*port*]

Syntax Definitions

<i>options</i>	Enter a question mark (?) to get a list of options.
<i>host</i>	Specifies the IP address of the TFTP server.
<i>port</i>	Specifies the port for the TFTP transfer.

Defaults

- If a path is not specified with the filename, the current path is used by default (for example, /flash).
- If a local filename is not specified, the remote filename is used by default.

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The OmniSwitch supports TFTP client functionality only.
- A TFTP server has no provisions for user authentication.
- When downloading a file to the switch, the file size must not exceed the available flash space.

Examples

```
-> tftp -g -l local_file -r remote_file 198.51.100.100
```

Release History

Release 7.1.1; command was introduced.

Related Commands

<code>cd</code>	Changes the current working directory of the switch.
<code>pwd</code>	Displays the current working directory of the switch.
<code>ls</code>	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
  systemServicesArg1
  systemServicesArg2
  systemServicesArg3
  systemServicesArg4
  systemServicesArg5
  systemServicesAction
```

sftp

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

sftp [*options*] {*host_name* | *ip_address*}

Syntax Definitions

<i>options</i>	Press “Enter” on the command line to get a list of options.
<i>host_name</i>	Specifies the host name for the SFTP session.
<i>ip_address</i>	Specifies the IPv4 or IPv6 address for the SFTP session.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You must have a valid username and a password for the specified host.
- After logging in, SFTP commands are supported. Some of these commands 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.
mkdir 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:
-> sftp
usage: sftp [-lCv] [-B buffer_size] [-b batchfile] [-F ssh_config]
          [-o ssh_option] [-P sftp_server_path] [-R num_requests]
          [-S program] [-s subsystem | sftp_server] host
sftp [[user@]host[:file [file]]]
sftp [[user@]host[:dir[/]]]
sftp -b batchfile [user@]host
```

Release History

Release 7.1.1; 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
```

ftp

Starts an FTP session.

```
ftp {port [default | service_port] | admin-state [enable | disable] | host_name | ip_address}  
[vrf name] ftp admin-state [enable | disable]
```

Syntax Definitions

<i>name</i>	The name of the VRF.
default	Sets the port back to the default of 21.
<i>service_port</i>	The TCP service port number. Must be 21 or between between 20000-20999.
enable disable	Enables or disables FTP access.
<i>host_name</i>	Specifies the host name for the FTP session.
<i>ip_address</i>	Specifies the IPv4 address for the FTP session.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- You must have a valid username and password for the specified host.
- The default FTP directory is **/flash**.

Examples

```
-> ftp port 20000  
-> ftp admin-state disable  
-> ftp 172.17.6.228  
-> vrf vrf1 ftp admin-state enable
```

Release History

Release 7.1.1; command introduced.

Release 7.3.1; **vrf** parameter added.

Related Commands

<code>cd</code>	Changes the current working directory of the switch.
<code>pwd</code>	Displays the current working directory of the switch.
<code>ls</code>	Displays the contents of a specified directory or the current working directory.

MIB Objects

```
systemServices
  systemServicesArg1
  systemServicesAction
  alaIpFtpAdminStatus
```

51 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:

[webview server](#)
[webview access](#)
[webview force-ssl](#)
[webview http-port](#)
[webview https-port](#)
[show webview](#)

webview server

Enables or disables the web management server on the switch.

[vrf name] webview server enable

[vrf name] webview server disable

Syntax Definitions

name The name of the VRF.

enable | disable Enables or disables the web management server on the switch.

Defaults

parameter	default
WebView Server	Enabled

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If the WebView Server is disabled, WebView Access is automatically disabled.
- VRF name must either be 'default' or pre-defined VRF (user-defined).

Examples

```
-> webview server enable
-> webview server disable
-> vrf vrf1 webview server enable
```

Release History

Release 7.1.1; command was introduced.

Release 7.3.1; **vrf** parameter added.

Related Commands

[webview access](#) Enables/disables webview access on the switch.

[show webview](#) Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
  alaInd1WebMgtServerStatus
```

webview access

Enables or disables web management access on the switch.

[vrf name] webview access enable

[vrf name] webview access disable

Syntax Definitions

name

The name of the VRF.

enable | disable

Enables or disables web management access on the switch.

Defaults

parameter	default
WebView Access	Enabled

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If Web Access is enabled, the WebView Server is automatically enabled.
- VRF name must either be 'default' or pre-defined VRF (user-defined).

Examples

```
-> webview access enable
-> webview access disable
-> vrf vrf1 webview access enable
```

Release History

Release 7.1.1; command was introduced.

Release 7.3.1; **vrf** parameter added.

Related Commands

[webview server](#)

Enables/disables the web server on the switch.

[show webview](#)

Displays web management configuration information.

MIB Objects

alaIND1WebMgtConfigMIBGroup

alaInd1WebMgtAdminStatus

webview force-ssl

Enables/disables Force SSL on the switch. SSL is a protocol that establishes and maintains secure communication between SSL-enabled servers and clients.

webview force-ssl enable

webview force-ssl disable

Syntax Definitions

enable | disable

Enabling this feature forces the user to use ssl to access the switch when using WebView.

Defaults

parameter	default
Force SSL	Enabled

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

The switch contains a self-signed certificate that may prompt a certificate warning.

Examples

```
-> webview force-ssl enable  
-> webview force-ssl disable
```

Release 7.1.1; command was introduced.

Related Commands

[webview access](#)

Enables/disables webview access on the switch.

[show webview](#)

Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup  
alaInd1WebMgtSsl
```

webview http-port

Changes the port number for the embedded web management server.

```
webview http-port {default | port port}
```

Syntax Definitions

default	Restores the port to its default (80) value.
<i>port</i>	The desired port number for the embedded Web server. The number must be in the range 0 to 65535; well-known port numbers cannot be configured.

Defaults

parameter	default
<i>port</i>	80

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

All WebView sessions must be terminated before entering this command.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
  alaIND1WebMgtHttpPort
```

webview https-port

Changes the default secure (HTTPS) port for the embedded web management server.

```
webview https-port {default | port port}
```

Syntax Definitions

default	Restores the port to its default (443) value.
<i>port</i>	The desired HTTPS port number. The number must be in the range 0 to 65535; well-known port numbers cannot be configured.

Defaults

parameter	default
<i>port</i>	443

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

All WebView sessions must be terminated before entering this command.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

webview access	Enables/disables webview access on the switch.
show webview	Displays web management configuration information.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup  
  alaIND1WebMgtHttpsPort
```

Release History

Release 7.1.1; command was introduced.

Release 7.3.1; `vrf` parameter added.

Related Commands

webview server	Enables/disables web management server on the switch.
webview access	Enables/disables webview access on the switch.
webview force-ssl	Enables/disables SSL on the switch.

MIB Objects

```
alaIND1WebMgtConfigMIBGroup
  alaInd1WebMgtServerStatus
  alaInd1WebMgtAdminStatus
  alaInd1WebMgtSsl
  alaInd1WebMgtHttpPort
  alaInd1WebMgtHttpsPort
```

52 Configuration File Manager Commands

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

MIB information for the Configuration Manager commands is as follows:

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

A summary of the available commands is listed here:

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

configuration apply

Applies a configuration file to the switch. Files may be applied immediately or after a designated timer session. With the timer session option, files are applied either at a scheduled date and time or after a specified period of time (i.e., a countdown) has passed.

configuration apply *filename* [**at** *hh:mm month dd* [*year*]] | [**in** *hh[:mm]*] [**verbose**]

Syntax Definitions

<i>filename</i>	The name of the configuration text file to be applied to the switch (e.g., newfile1).
at <i>hh:mm</i> { <i>dd month / month dd</i> } [<i>year</i>]	Designates a timer session in which a configuration file is applied at a specified date and time in the future. Values for <i>hh</i> range from 00 through 23. Values for <i>mm</i> range from 00 through 59. Values for <i>dd</i> 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 <i>hh[:mm]</i>	Designates a timer session in which the configuration file is applied after a specific amount of time (i.e., a countdown) has passed. Values for <i>hh</i> range from 00 through 23. Values for <i>mm</i> 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 10K, 6900

Usage Guidelines

- The **configuration apply** command only applies settings to the running configuration. The **boot.cfg** file does not get overwritten.
- It is recommended that you check all configuration files for syntax errors before applying them to your switch.
- To schedule a timer session in which a file is applied at a specific date and time, enter **at** followed by the hour, minute, month, day, and year. The switch assumes either the current calendar year or the next calendar year for dates beginning January 1.
- To schedule a timer session in which a file is applied after a specific amount of time (i.e., a countdown) has passed, enter **in** followed by the number of hours and minutes.
- Verbose mode is not supported for timer sessions.

- The keyword, **authkey**, along with a related alpha-numeric text string, are automatically included in many snapshot files (e.g., **configuration snapshot all**). The text string following the **authkey** keyword represents a login password that has been encrypted *twice*. (The first encryption occurs when a password is first created by a user; the second encryption occurs when a configuration snapshot is taken.) This dual encryption further enhances switch security. However, it is important to note that any configuration file (including a generated snapshot) that includes this dual-encrypted password information will result in an error whenever it is applied to the switch via the **configuration apply** command. This is a valid switch function and does not represent a significant problem. If an **authkey**-related error is the *only* error detected, simply remove all **authkey**-related syntax using a text editor. If a new password is required for the switch, include valid password syntax in the configuration file or immediately issue a new password by using the **password** command at the command prompt. For more information on passwords, refer to [page 31-24](#).

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 7.1.1; command was introduced.

Related Commands

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

MIB Objects

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

configuration error-file-limit

Specifies the maximum number of configuration error files allowed in the switch's **/flash** directory. Error files are normally generated when a configuration file is applied to the switch. Error files are identified by their **.err** extension. When the maximum number of **.err** files is exceeded, any new error file will overwrite 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
<i>number</i>	1

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When the error file limit is set to 1 (the default value), the next error file generated by the switch will replace the existing one.
- When the error file limit is set to a value greater than 1, when a new error file that exceeds the maximum limit is created, the switch will automatically remove the error file with the smallest timestamp.
- The error files generated by the switch have the **.err** extension.
- If you want to save an error file, you may change the file name so that it does not have the **.err** extension, or you can move it from the **/flash** directory.

Examples

```
-> configuration error-file-limit 2
-> configuration error-file-limit 1
```

Release History

Release 7.1.1; command was introduced.

Related Commands

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

MIB Objects

alcatelIND1ConfigMgrMIBObjects
configErrorFileMaximum

show configuration status

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

show configuration status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- A timer session can be scheduled using the [configuration apply](#) command. For more information, refer to [page 52-2](#).
- The screen output **File configuration </path/filename>: scheduled at dd/mm hh:mm** indicates that a timer session has been scheduled for a later time.
- The output **No file configuration has been scheduled** indicates an idle timer session (i.e., no timer session has been scheduled for a configuration file).
- The output **File configuration is in progress** indicates that a file is currently being applied to the switch.
- The output **File configuration </path/filename>: completed with 2 errors** indicates that the named file was applied to the switch with two recorded errors.
- When the running and saved configurations are the same, the output **Running configuration and saved configuration are identical** will be displayed.
- When the running and saved configurations are the different, the output **Running configuration and saved configuration are different** will be displayed.
- To synchronize the running and saved configuration, use the [issu slot](#) command.

Examples

```
-> show configuration status
```

Release History

Release 7.1.1; 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.
- issu slot** 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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> configuration cancel
```

Release History

Release 7.1.1; command was introduced.

Related Commands

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

show configuration status Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

```
configTimerFileGroup  
configTimerClear
```

configuration syntax-check

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

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

Syntax Definitions

path/filename

The configuration file being checked for syntax and authorization errors. If a configuration file is located in another directory, be sure to specify the full path. For example, **/flash/working/asc.1.snap**.

verbose

When **verbose** is specified in the command line, all syntax contained in the configuration file is printed to the console, even if no error is detected. When **verbose** is *not* specified in the command line, cursory information (number of errors and error log file name) will be printed to the console *only if a syntax or configuration error is detected*.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- When an error is detected, an error file (**.err**) is automatically generated by the switch. By default, this file is placed in the root **/flash** directory. To view the contents of a generated error file, use the **view** command. For example, **view asc.1.snap.1.err**.
- The syntax, **mac alloc**, is automatically included in many snapshot files (e.g., **configuration snapshot all**). All **mac alloc**-related syntax is valid *during switch boot up only* (i.e., it cannot be applied while the switch is in run-time operation). Because snapshot files are commonly used as configuration files, syntax checks may detect **mac alloc** syntax and issue an error (along with a generated **.err** file). This is a valid switch function and does not represent a significant problem. If a **mac alloc**-related error is the *only* error detected, simply remove the syntax using a text editor, then re-check the file using the **configuration syntax-check** command.
- It is recommended that you check all configuration files for syntax errors before applying them to your switch.

Examples

```
-> configuration syntax-check vlan_file1  
..
```

Note. When the **configuration syntax-check** command is entered, one or more dots “.” is displayed in the command output. This indicates command progress; each dot represents 256 text lines in the configuration file processed by the syntax check mechanism.

Release History

Release 7.1.1; 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	ipmr	rdp
aaa	ipms	rip
aip	ipx	ripng
all	ipv6	session
bgp	linkagg	slb
bridge	module	snmp
chassis	ntp	stp
health	ospf	system
interface	ospf3	vlan
ip	pmm	vrrp
ip-helper	policy	webmgt
ip-routing	qos	udld
netsec		

path/filename

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

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

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

show configuration snapshot

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

show configuration snapshot [*feature_list*]

Syntax Definitions

feature_list

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

snapshot-supported features

802.1q	ipmr	rdp
aaa	ipms	rip
aip	ipx	ripng
all	ipv6	session
bgp	linkagg	slb
bridge	module	snmp
chassis	ntp	stp
health	ospf	system
interface	ospf3	vlan
ip	pmm	vrrp
ip-helper	policy	webmgt
ip-routing	qos	udld
netsec		

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use this command to view the current configuration for any feature shown in the table.
- To show a list of features on the switch, use the **show configuration snapshot ?** syntax.
- Configurations are listed below the name of each feature.
- Features with no current configuration show only the name of the feature.

Examples

```
-> show configuration snapshot
-> show configuration snapshot aaa bridge
! Bridging :

! AAA :
aaa authentication default "local"
aaa authentication console "local"
user "public" read All write All no auth authkey 391b0e74dbd13973d703ccea4a8e30
```

Release History

Release 7.1.1; command was introduced.

Related Commands

[write terminal](#) Displays the switch's current running configuration for all features.

MIB Objects

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

write terminal

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

write terminal

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
```

53 SNMP Commands

This chapter includes descriptions for Trap Manager and SNMP Agent commands. The commands are used for configuring SNMP settings on the switch.

- SNMP station commands can create, modify, or delete an SNMP station. Also included is a show command for monitoring current SNMP station status.
- SNMP trap commands configure SNMP trap settings. Traps can be replayed and filtered. Also, test traps can be generated to verify that individual traps are being correctly handled by the Network Management Station (NMS). The SNMP trap commands set includes show commands for monitoring SNMP trap information.
- SNMP agent commands configure SNMP security levels on the switch. Also includes show commands for monitoring the current SNMP security status.

MIB information for SNMP Community commands is as follows:

Filename: IETFsnmpCommunity.MIB
Module: IETF SNMP-COMMUNITY.MIB

MIB information for Trap Manager commands is as follows:

Filename AlcatelIND1TrapMgr.MIB
Module: ALCATEL-IND1-TRAP-MGR.MIB

MIB information for SNMP Agent commands is as follows:

Filename: AlcatelIND1SNMPAgent.MIB
Module: ALCATEL-IND1-SNMP-AGENT.MIB

A summary of the available commands is listed here:

SNMP station commands	snmp station show snmp station
SNMP community map commands	snmp community-map snmp community-map mode show snmp community-map
SNMP security commands	snmp security show snmp security show snmp statistics show snmp mib-family
SNMP trap commands	snmp-trap absorption snmp-trap to-webview snmp-trap replay-ip snmp-trap filter-ip snmp authentication-trap show snmp-trap replay-ip show snmp-trap filter-ip show snmp authentication-trap show snmp-trap config

snmp station

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

snmp station {*ip_address* | *ipv6_address*} [[*udp_port*] [*username*] [**v1** | **v2** | **v3**] [**enable** | **disable**]]

no snmp station {*ip_address* | *ipv6_address*}

Syntax Definitions

<i>ip_address</i>	The IP address to which SNMP unicast traps will be sent.
<i>ipv6_address</i>	The IPv6 address to which SNMP unicast traps will be sent.
<i>udp_port</i>	A UDP destination port.
<i>username</i>	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
<i>udp_port</i>	162
v1 v2 v3	v3
enable disable	enable

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the no form of the command to remove an existing SNMP station.
- When adding an SNMP station, you must specify an IP address *plus username parameters*. For example, the syntax **snmp station 1.2.3.4** is not a valid command entry; however, **snmp station 1.2.3.4 username1** is a valid command entry.
- When modifying an SNMP station, you must specify an IP address *plus at least one additional parameter*. For example, the syntax **snmp station 1.2.3.4** is not a valid command entry; however, **snmp station 1.2.3.4 v2** is a valid command entry.
- 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 7.1.1; 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
```

show snmp station

Displays the current SNMP station status.

show snmp station

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show snmp station
ipAddress/udpPort          status    protocol user
-----
199.199.100.200/8010      enable   v3       NMSuserV3MD5DES
199.199.101.201/111      disable  v2       NMSuserV3MD5
199.199.102.202/8002      enable   v1       NMSuserV3SHADES
199.199.103.203/8003      enable   v3       NMSuserV3SHADES
199.199.104.204/8004      enable   v3       NMSuserV3SHA
```

output definitions

IPAddress	IP Address of the SNMP management station.
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 7.1.1; 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

<i>community_string</i>	A community string in the form of a text string. This string must be between 1 and 32 characters.
<i>useraccount_name</i>	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 10K, 6900

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.
- The community-map mode must be enabled and 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.

Examples

```
-> snmp community-map community1 user testname1  
-> snmp community-map community1 enable
```

Release History

Release 7.1.1; 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

parameter	default
Community mode	disabled

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- The community-map mode must be enabled and the community string carried over each incoming v1 or v2c SNMP request must be mapped to a user account name with SNMP privileges 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.

Examples

```
-> snmp community-map mode enable  
-> snmp community-map mode disable
```

Release History

Release 7.1.1; 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 10K, 6900

Usage Guideline

N/A

Examples

```
-> show snmp community-map
Community mode : enabled
```

```
status  community string          user name
-----+-----+-----+-----
enabled test_string1             bb_username
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 7.1.1; command was introduced.

Related Commands

[snmp community-map](#) Configures and enables a community string on the switch and maps it to an existing user account name.

snmp security

Configures SNMP security settings.

snmp security {no-security | authentication set | authentication all | privacy set | privacy all | trap-only}

Syntax Definitions

no-security	The switch will accept all SNMP v1, v2, and v3 requests.
authentication set	The switch will accept all requests <i>except</i> v1, v2, and non-authenticated v3 set requests. SNMP v1, v2, and non-authenticated v3 set requests will be rejected.
authentication all	The switch will accept all requests <i>except</i> v1, v2, and non-authenticated v3 get, get-next, and set requests. SNMP v1, v2, and non-authenticated v3 get, get-next, and set requests will be rejected.
privacy set	The switch will accept <i>only</i> authenticated SNMP v3 get, get-next and encrypted v3 set requests. All other requests will be rejected.
privacy all	The switch will accept only encrypted v3 get, get-next, and set requests. All other requests will be rejected.
trap-only	All SNMP get, get-next, and set requests will be rejected.

Defaults

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

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

Usage Guidelines

Refer to the command on page [53-11](#) for descriptions of the five SNMP security states: no security, authentication set, authentication all, privacy set, privacy all, and trap only.

Examples

```
-> show snmp security  
snmp security = no security
```

```
-> show snmp security  
snmp security = authentication set
```

```
-> show snmp security  
snmp security = authentication all
```

```
-> show snmp security  
snmp security = privacy set
```

```
-> show snmp security  
snmp security = privacy all
```

```
-> show snmp security  
snmp security = trap only
```

Release History

Release 7.1.1; command was introduced.

Related Commands[snmp security](#)Configures the SNMP security settings.

show snmp statistics

Displays the current SNMP statistics.

show snmp statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; command was introduced.

Related Commands

N/A

show snmp mib-family

Displays SNMP MIB information. Information includes MIP ID number, MIB table name, and command family.

show snmp mib-family [*table_name*]

Syntax Definitions

table_name The name of the MIB table to be displayed.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- If a table name is not specified in the command syntax, all MIB table names will be displayed.
- If the command family is not valid for the entire MIB table, the command family will be displayed on a per-object basis.
- Table names are case-sensitive. Therefore, use the exact table names from the MIB database.

Examples

```
-> show snmp mib-family trapStationTable
MIP ID   MIB TABLE NAME                               FAMILY
-----+-----+-----
 73733   trapStationTable                             snmp
```

output definitions

MIP ID	Identification number for the MIP associated with this MIB Table.
MIB Table Name	Name of the MIB table.
Family	Command family to which this MIB table belongs.

Release History

Release 7.1.1; command was introduced.

Related Commands

[show snmp-trap filter-ip](#) Displays the SNMP trap filter information.

snmp-trap absorption

Enables or disables the trap absorption function.

snmp-trap absorption {enable | disable}

Syntax Definitions

enable	Enables SNMP trap absorption. When trap absorption is enabled, identical, repetitive traps sent by applications during a pre-configured time period will be absorbed, and therefore not sent to SNMP Manager stations configured on the switch.
disable	Disables SNMP trap absorption.

Defaults

By default, trap absorption is enabled.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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 10K, 6900

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 7.1.1; 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-ip

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 {ip_address | ipv6_address} [seq_id]
```

Syntax Definitions

<i>ip_address</i>	The IP address for the SNMP station to which traps will be replayed from the switch.
<i>ipv6_address</i>	The IPv6 address for the SNMP station to which traps will be replayed from the switch.
<i>seq_id</i>	The sequence number from which trap replay will begin. Each trap sent by the switch to an SNMP station has a sequence number. The sequence number reflects the order in which the trap was sent to the SNMP station. For example, the first trap sent to an SNMP station has a sequence number of 1; the second trap has a sequence number of 2, etc. If no sequence number is entered, all stored traps are replayed.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

- Use the [show snmp station](#) command on [page 53-5](#) to display the latest stored sequence number for each SNMP station.
- The switch replays traps in the same order that they were previously sent, beginning from the specified sequence number.
- When traps are replayed, the original dates on which the trap was issued, rather than the current dates are used.
- If the specified sequence number is lower than the oldest trap sequence number stored in the switch, the switch replays all stored traps.
- If the specified sequence number is equal to or greater than the oldest trap sequence number stored, the switch replays all stored traps from the specified sequence number up to the latest sequence number.
- If the specified sequence number is greater than the latest sequence number, no traps are replayed.

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

- | | |
|--|--|
| show snmp station | Displays the current SNMP station status. |
| show snmp-trap replay-ip | Displays the SNMP trap replay information. |

MIB Objects

```
trapStationTable
  trapStation Replay
AlaTrapInetStationEntry
  alaTrapInetStationReplay
  alaTrapInetStationNextSeq
```

snmp-trap filter-ip

Enables or disables SNMP trap filtering. Trap filtering is used to determine whether a trap or group of traps will be sent from the switch to a specified SNMP station.

snmp-trap filter-ip {*ip_address* | *ipv6_address*} *trap_id_list*

no snmp-trap filter-ip {*ip_address* | *ipv6_address*} *trap_id_list*

Syntax Definitions

<i>ip_address</i>	The IP address for the SNMP station for which trap filtering is being enabled or disabled.
<i>ipv6_address</i>	The IPv6 address for the SNMP station for which trap filtering is being enabled or disabled.
<i>trap_id_list</i>	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 10K, 6900

Usage Guidelines

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

Examples

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

Release History

Release 7.1.1; command was introduced.

Related Commands

show snmp-trap filter-ip

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 10K, 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; 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-ip

Displays SNMP trap replay information.

```
show snmp-trap replay-ip
```

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show snmp-trap replay-ip
ipAddress      : oldest replay number
-----
199.199.101.200 :      1234
199.199.105.202 :       578
199.199.101.203 :     1638
199.199.101.204 :     2560
```

output definitions

IPAddress	IP address of the SNMP station manager that replayed the trap.
Oldest Replay Number	Number of the oldest replayed trap.

Release History

Release 7.1.1; command was introduced.

Related Commands

[snmp-trap replay-ip](#)

Replays stored traps from the switch to a specified SNMP station.

MIB Objects

trapStationTable

 snmpStation Replay

AlaTrapInetStationEntry

 alaTrapInetStationReplay

 alaTrapInetStationNextSeq

show snmp-trap filter-ip

Displays the current SNMP trap filter status.

show snmp-trap filter-ip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

To display a list of traps and their ID numbers, use the [show snmp-trap config](#) command.

Examples

```
-> show snmp-trap filter-ip
ipAddress      : trapId list
-----
199.199.101.200 :    0  1  2  3
199.199.101.201 : no filter
199.199.105.202 :    0  1  2  3  4  5  6  7  8  9 10 11 12 13 14
                  15 16 17 18 19
199.199.101.203 :   20 22 30
199.199.101.204 : no filter
```

output definitions

IPAddress	IP address of the SNMP management station that recorded the traps.
TrapId List	Identification number for the traps being filtered.

Release History

Release 7.1.1; command was introduced.

Related Commands

[snmp-trap filter-ip](#)

Enables or disables SNMP trap filtering.

[show snmp-trap config](#)

Displays the SNMP trap information, including trap ID numbers, trap names, command families, and absorption rate.

MIB Objects

trapFilterTable

 trapFilterEntry

alaTrapInetFilterTable

 alaTrapInetFilterStatus

show snmp authentication-trap

Displays the current authentication failure trap forwarding status (i.e., enable or disable).

show snmp authentication-trap

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

Usage Guidelines

N/A

Examples

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

Release History

Release 7.1.1; 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 10K, 6900

Usage Guidelines

N/A

Examples

```
-> show snmp-trap config
Absorption service : enabled
Traps to WebView : enabled
```

Id	trapName	family	absorption
0	coldStart	chassis	15 seconds
1	warmStart	chassis	15 seconds
2	linkDown	interface	15 seconds
3	linkUp	interface	15 seconds
4	authenticationFailure	snmp	15 seconds
5	entConfigChange	module	15 seconds
30	slPesudoCAMStatusTrap	bridge	15 seconds
31	slbTrapException	loadbalancing	15 seconds
32	slbTrapConfigChanged	loadbalancing	15 seconds
33	slbTrapOperStatus	loadbalancing	15 seconds
34	ifMauJabberTrap	interface	15 seconds
35	sessionAuthenticationTrap	session	15 seconds

output definitions

Id	Identification number for the trap.
Trap Name	Name of the trap.
Family	Family to which the trap belongs.
Absorption	Time needed for the trap to process.

Release History

Release 7.1.1; 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

54 DNS Commands

A Domain Name System resolver is an internet service that translates host names into IP addresses. Every time you use a host name, a DNS service must resolve the name to an IP address. You can configure up to three domain name servers. If the primary DNS server does not know how to translate a particular host name, it asks the secondary DNS server (if specified). If this fails, it asks the third DNS server (if specified), until the correct IP address is returned (resolved). If all DNS servers have been queried and the name is still not resolved to an IP address, the DNS resolver will fail and issue an error message.

MIB information for the DNS commands is as follows:

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

A summary of the available commands is listed here.

[ip domain-lookup](#)
[ip name-server](#)
[ipv6 name-server](#)
[ip domain-name](#)
[show dns](#)

ip domain-lookup

Enables or disables the DNS resolver.

ip domain-lookup

no ip domain-lookup

Syntax Definitions

N/A

Defaults

By default, the DNS resolver is disabled.

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>server-address1</i>	The IP address of the primary DNS server to query for host lookup. This is the only address that is required.
<i>server-address2</i>	The IP address of the secondary DNS server to query for host lookup. This server will be queried only if the desired host name or host IP address is not located by the primary DNS server. A second IP address is optional.
<i>server-address3</i>	The IP address of the DNS server with the lower priority. This server will be queried only if the desired host name or IP address is not located by the primary and secondary DNS servers. A third IP address is optional.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

<i>server-ipv6_address1</i>	The IPv6 address of the primary IPv6 DNS server to query for host lookup. Specifying the primary IPv6 DNS address is mandatory.
<i>server-ipv6_address2</i>	The IPv6 address of the secondary IPv6 DNS server to query for host lookup. This server will be queried only if the desired host name is not able to be resolved by the primary IPv6 DNS server. A second IPv6 address is optional.
<i>server-ipv6_address3</i>	The IPv6 address of the IPv6 DNS server with the lower priority. This server will be queried only if the desired host name is not able to be resolved by both the primary and secondary IPv6 DNS servers. A third IPv6 address is optional.

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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

show dns

Displays the current DNS resolver configuration and status.

show dns

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 10K, 6900

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 7.1.1; 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
```

A Software License and Copyright Statements

This appendix contains Alcatel-Lucent and third-party software vendor license and copyright statements.

Alcatel-Lucent License Agreement

ALCATEL-LUCENT SOFTWARE LICENSE AGREEMENT

IMPORTANT. Please read the terms and conditions of this license agreement carefully before opening this package.

By opening this package, you accept and agree to the terms of this license agreement. If you are not willing to be bound by the terms of this license agreement, do not open this package. Please promptly return the product and any materials in unopened form to the place where you obtained it for a full refund.

1. **License Grant.** This is a license, not a sales agreement, between you (the “Licensee”) and Alcatel-Lucent. Alcatel-Lucent hereby grants to Licensee, and Licensee accepts, a non-exclusive license to use program media and computer software contained therein (the “Licensed Files”) and the accompanying user documentation (collectively the “Licensed Materials”), only as authorized in this License Agreement. Licensee, subject to the terms of this License Agreement, may use one copy of the Licensed Files on the Licensee’s system. Licensee agrees not to assign, sublicense, transfer, pledge, lease, rent, or share their rights under this License Agreement. Licensee may retain the program media for backup purposes with retention of the copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Licensed Materials or any portions thereof may be made by Licensee and Licensee shall not modify, decompile, disassemble, reverse engineer, or otherwise attempt to derive the Source Code. Licensee is also advised that Alcatel-Lucent products contain embedded software known as firmware which resides in silicon. Licensee may not copy the firmware or transfer the firmware to another medium.

2. **Alcatel-Lucent’s Rights.** Licensee acknowledges and agrees that the Licensed Materials are the sole property of Alcatel-Lucent and its licensors (herein “its licensors”), protected by U.S. copyright law, trademark law, and are licensed on a right to use basis. Licensee further acknowledges and agrees that all rights, title, and interest in and to the Licensed Materials are and shall remain with Alcatel-Lucent and its licensors and that no such right, license, or interest shall be asserted with respect to such copyrights and trademarks. This License Agreement does not convey to Licensee an interest in or to the Licensed Materials, but only a limited right to use revocable in accordance with the terms of this License Agreement.

3. **Confidentiality.** Alcatel-Lucent considers the Licensed Files to contain valuable trade secrets of Alcatel-Lucent, the unauthorized disclosure of which could cause irreparable harm to Alcatel-Lucent. Except as expressly set forth herein, Licensee agrees to use reasonable efforts not to disclose the Licensed Files to any third party and not to use the Licensed Files other than for the purpose authorized by this License Agreement. This confidentiality obligation shall continue after any termination of this License Agreement.

4. **Indemnity.** Licensee agrees to indemnify, defend and hold Alcatel-Lucent harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation Alcatel-Lucent's reasonable United States and local attorneys' and expert witnesses' fees and costs) arising out of or in connection with the unauthorized copying, marketing, performance or distribution of the Licensed Files.

5. **Limited Warranty.** Alcatel-Lucent warrants, for Licensee's benefit alone, that the program media shall, for a period of ninety (90) days from the date of commencement of this License Agreement (referred to as the Warranty Period), be free from defects in material and workmanship. Alcatel-Lucent further warrants, for Licensee benefit alone, that during the Warranty Period the Licensed Files shall operate substantially in accordance with the functional specifications in the User Guide. If during the Warranty Period, a defect in the Licensed Files appears, Licensee may return the Licensed Files to Alcatel-Lucent for either replacement or, if so elected by Alcatel-Lucent, refund of amounts paid by Licensee under this License Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE LICENSED MATERIALS ARE LICENSED "AS IS" AND ALCATEL-LUCENT AND ITS LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. THIS WARRANTY GIVES THE LICENSEE SPECIFIC LEGAL RIGHTS. LICENSEE MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

6. **Limitation of Liability.** Alcatel-Lucent's cumulative liability to Licensee or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the license fee paid to Alcatel-Lucent for the Licensed Materials. IN NO EVENT SHALL ALCATEL-LUCENT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF ALCATEL-LUCENT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION TO INCIDENTAL OR CONSEQUENTIAL DAMAGES MAY NOT APPLY TO LICENSEE.

7. **Export Control.** This product is subject to the jurisdiction of the United States. Licensee may not export or reexport the Licensed Files, without complying with all United States export laws and regulations, including but not limited to (i) obtaining prior authorization from the U.S. Department of Commerce if a validated export license is required, and (ii) obtaining "written assurances" from licensees, if required.

8. **Support and Maintenance.** Except as may be provided in a separate agreement between Alcatel-Lucent and Licensee, if any, Alcatel-Lucent is under no obligation to maintain or support the copies of the Licensed Files made and distributed hereunder and Alcatel-Lucent has no obligation to furnish Licensee with any further assistance, documentation or information of any nature or kind.

9. **Term.** This License Agreement is effective upon Licensee opening this package and shall continue until terminated. Licensee may terminate this License Agreement at any time by returning the Licensed Materials and all copies thereof and extracts therefrom to Alcatel-Lucent and certifying to Alcatel-Lucent in writing that all Licensed Materials and all copies thereof and extracts therefrom have been returned or erased by the memory of Licensee's computer or made non-readable. Alcatel-Lucent may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by

Alcatel-Lucent, Licensee agrees to return to Alcatel-Lucent or destroy the Licensed Materials and all copies and portions thereof.

10. Governing Law. This License Agreement shall be construed and governed in accordance with the laws of the State of California.

11. Severability. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms herein.

12. No Waiver. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

13. Notes to United States Government Users. Software and documentation are provided with restricted rights. Use, duplication or disclosure by the government is subject to (i) restrictions set forth in GSA ADP Schedule Contract with Alcatel-Lucent's reseller(s), or (ii) restrictions set forth in subparagraph (c) (1) and (2) of 48 CFR 52.227-19, as applicable.

14. Third Party Materials. Licensee is notified that the Licensed Files contain third party software and materials licensed to Alcatel-Lucent by certain third party licensors. Some third party licensors are third party beneficiaries to this License Agreement with full rights of enforcement. Please refer to the section entitled "[Third Party Licenses and Notices](#)" on page -4 for the third party license and notice terms.

Third Party Licenses and Notices

Legal Notices applicable to any software distributed alone or in connection with the product to which this document pertains, are contained in files within the software itself located at: **/flash/foss**.

Also, if needed, we provide all FOSS (Free and Open Source Software) source code used into this release at the following URL: <https://service.esd.alcatel-lucent.com/portal/page/portal/EService/release>

B CLI Change Guidelines

This appendix provides general guidelines for determining the CLI changes from AOS Release 6 to AOS Release 7. In addition, a summary of AOS Release 7 CLI command shortcuts is provided (see [“OmniSwitch CLI Short Cuts” on page B-29](#)).

For detailed explanations regarding commands and parameters, refer to the appropriate chapter in the *OmniSwitch CLI Reference Guide*.

AOS Release 6 to AOS Release 7

List of Changed CLI Commands

“AAA Commands”	“OSPF Commands”
“BFD Commands”	“OSPFv3 Commands”
“BGP Commands”	“PIM Commands”
“Configuration File Manager Commands”	“Port Security Commands”
“Chassis Management and Monitoring Commands”	“Policy Server Commands”
“CMM Commands”	“Port Manager Commands”
“DHCP Relay Commands”	“Port Mapping Commands”
“DVMRP Commands”	“Port Mirroring and Monitoring Commands”
“ERP Commands”	“QoS Commands”
“Ethernet Port Commands”	“RIP Commands”
“Health Monitor Commands”	“Sflow Commands”
“HTTP Commands”	“SLB Commands”
“IPsec Commands”	“SNMP Commands”
“IPv4 Commands”	“Source Learning Commands”
“IPv6 Commands”	“STP Commands”
“Link Aggregation Commands”	“System Services Command”
“802.1AB Commands”	“VLAN Manager Commands”
“Multicast Routing Commands”	“VLAN Stacking Commands”
“Network Time Protocol Commands”	“VRRP Commands”

AAA Commands

AOS Release 6	AOS Release 7
aaa radius agent preferred {default no-loopback <ip_address>}	removed
no aaa radius agent preferred	removed
user <i>user_name</i> end-user-profile <string>	removed
user <i>user_name</i> no end-user-profile	removed
end-user profile	removed
no end-user profile	removed
show end-user profile	removed
show user password-expiration	removed
show user password-size	removed
aaa radius-agent	removed
aaa ace-server	removed

BFD Commands

AOS Release 6	AOS Release 7
ip bfd-std status {enable disable}	ip bfd admin-state {enable disable}
ip bfd-std transmit-interval	ip bfd transmit <i>transmit_interval</i>
ip bfd-std receive receive-interval	ip bfd receive <i>receive_interval</i>
ip bfd-std mode {echo-only demand echo {enable disable} asynchronous echo {enable disable}}	ip bfd mode {echo-only demand [echo-state {enable disable}] asynchronous [echo-state {enable disable}]}
ip bfd-std echo status {enable disable}	ip bfd echo-state {enable disable}
ip bfd-std echo interval echo-interval	ip bfd echo-interval <i>echo_interval</i>
ip bfd-std 12-hold-timer 12-holdtimer-interval	ip bfd 12-hold-timer <i>12-holdtimer-interval</i>
ip bfd-std interface interface_name	ip bfd interface <i>if_name</i>
no ip bfd-std interface interface_name	no ip bfd interface <i>if_name</i>
ip bfd-std interface interface_name status {enable disable}	ip bfd interface <i>if_name</i> admin-state {enable disable}
ip bfd-std interface interface_name transmit transmit-interval	ip bfd interface <i>if_name</i> transmit <i>transmit_interval</i>
ip bfd-std interface interface_name receive receive-interval	ip bfd interface <i>if_name</i> receive <i>receive_interval</i>
ip bfd-std interface interface_name multiplier multiplier_value	ip bfd interface <i>if_name</i> multiplier <i>num</i>
ip bfd-std interface interface_name echo-interval echo-interval	ip bfd interface <i>if_name</i> echo-interval <i>echo_interval</i>

AOS Release 6	AOS Release 7
ip bfd-std interface interface_name mode {echo-only demand [echo {enable disable}] asynchronous [echo {enable disable}]}	ip bfd interface <i>interface_name</i> mode {echo-only demand [echo-state {enable disable}] asynchronous [echo-state {enable disable}]}
ip bfd-std interface interface_name 12-hold-timer 12-holdtimer-interval	ip bfd interface <i>interface_name</i> 12-hold-timer <i>12-holdtimer-interval</i>
ip ospf bfd-std status {enable disable}	ip ospf bfd-state {enable disable}
[no] ip ospf bfd-std all-interfaces	ip ospf bfd-state all-interfaces {enable disable}
ip ospf interface interface-name bfd-std {enable disable}	ip ospf interface <i>interface-name</i> bfd-state {enable disable}
ip ospf interface interface-name bfd-std drs-only	ip ospf interface <i>interface-name</i> bfd-state drs-only
ip ospf interface interface-name bfd-std all-nbrs	ip ospf interface <i>interface-name</i> bfd-state all-neighbors {enable disable}
ip bgp bfd-std status {enable disable}	ip bgp bfd-state {enable disable}
[no] ip bgp bfd-std all-neighbors	ip bgp bfd-state all-neighbors {enable disable}
ip bgp neighbor name bfd-std {enable disable}	ip bgp neighbor <i>ip_address</i> bfd-state {enable disable}
vrrp bfd-std {enable disable}	vrrp bfd-state {enable disable}
vrrp track num address address bfd-std {enable disable}	vrrp track <i>num</i> address <i>address</i> bfd-state {enable disable}
show ip bfd-std	show ip bfd
show ip bfd-std interfaces [interface-name]	show ip bfd interfaces [<i>if-name</i>]
show ip bfd-std [session <num>] [sessions [slot <num>]]	show ip bfd sessions [<i>session_num</i>] [slot <i>slot_num</i>]
n/a	ip bfd multiplier <i>num</i>
n/a	show ip bfd sessions statistics <i>session_num</i>
n/a	ip static-route <i>ipv4_prefix/pfx_length</i> gateway <i>ipv4_host_address</i> bfd-state {enable disable}

BGP Commands

AOS Release 6	AOS Release 7
ip bgp status {enable disable}	ip bgp admin-state {enable disable}
ip bgp network network_address ip_mask status {enable disable}	ip bgp network <network_address> <ip_mask> admin-state {enable disable}
ip bgp neighbor ip_address status {enable disable}	ip bgp neighbor <ip_address> admin-state {enable disable}
ipv6 bgp neighbor ipv6_address [status {enable disable}]	ipv6 bgp neighbor <ipv6_address> [admin-state {enable disable}]

Configuration File Manager Commands

AOS Release 6	AOS Release 7
show configuration snapshot [<appname>]	configuration apply <filename> [<time>]

Chassis Management and Monitoring Commands

AOS Release 6	AOS Release 7
n/a	hash-control load-balance non-ucast {enable disable}
n/a	show hash-control non-ucast
n/a	show escalation-strategy [<slot-id>]

CMM Commands

AOS Release 6	AOS Release 7
reload [primary secondary all] [with-fabric] [in [hours:] minutes at hour:minute [month day day month] cancel]	reload [primary secondary all] [in [hours:] minutes at hour:minute [month day day month] cancel]
reload working {rollback-timeout minutes no rollback-timeout} [in [hours:] minutes at hour:minute]	reload from <image-dir> {rollback-timeout minutes no rollback-timeout} [redundancy-time <redundancy-time>] [in [hours:] minutes at hour:minute]
n/a	issu from <image-dir> redundancy-time <redundancy-time>
[configure] copy running-config working	removed
[configure] copy certified working	copy certified <image-directory>
takeover [with-fabric]	takeover
show microcode [issu working certified loaded]	show microcode [issu working certified loaded <directory>]
show microcode history [working certified]	removed
system time-and-date synchro	removed
system timezone [timezone_abbrev offset_value time_notation]	system timezone [timezone_abbrev time_notation]
system daylight savings time [{enable disable} start {week} {day} in {month} at {hh:mm} end {week} {day} in {month} at {hh:mm} [by min]]	system daylight-savings-time
reload ni [slot] number	reload slot <number>
reload pass-through slot-number	removed
power ni [slot] slot-number	power slot <slot[-slot]>
no power ni [slot] slot-number	no power slot <slot[-slot]>
n/a	[no] powersupply enable [<psu-id>]

AOS Release 6	AOS Release 7
rdf	rdf [slot-nr]
rls <string> [<string>]	rls rem-slot <path> [<filename>]
rrm <string> <string>	rrm rem-slot <[path/]filename>
show cmm [number]	show cmm [<number> <cmm_letter>]
show ni [number]	show slot [<slot-nr>]
n/a	show transceivers [slot <slot-nr> [transceiver <transceiver_num>]]
show module [number]	show module [<number> <cmm_letter>]
show module long [number]	show module long [<number> <cmm_letter>]
show module status [number]	show module status [<number> <cmm_letter>]
show power [supply] [number]	show powersupply [<number>]
n/a	show fantray [<fantray-nr>]
show temperature [number]	show temperature [fabric [<index>] slot [<index>] fantray [<index>] cmm [<index> <cmm_letter>]]
show stack topology [slot-number]	removed
show stack status	removed
hash-control brief	moved to CapMan
hash-control extended [[no] udp-tcp-port]	moved to CapMan
show hash-control	moved to CapMan
n/a	show escalation-strategy [<slot-id>]
license apply	removed
show license info	removed
show license file	removed

DHCP Relay Commands

AOS Release 6	AOS Release 7
ip helper no address [ip_address]	no ip helper address <ip_address>*
ip helper address ip_address vlan vlan_id	ip helper vlan <vlan1[-vlan2]> address <ip_address>*
ip helper no address ip_address vlan vlan_id	no ip helper vlan <vlan1[-vlan2]> address <ip_address>*
ip helper avlan only	removed
ip helper forward delay seconds	ip helper forward-delay <seconds>
ip helper maximum hops hops	ip helper maximum-hops <hops>
ip helper traffic-suppression {enable disable}	removed
ip helper dhcp-snooping {enable disable}	removed

AOS Release 6	AOS Release 7
ip helper dhcp-snooping mac-address verification {enable disable}	removed
ip helper dhcp-snooping option-82 data-insertion {enable disable}	removed
ip helper dhcp-snooping option-82 data-insertion format {base-mac system-name userstring string interface-alias auto-interface-alias}	removed
ip helper dhcp-snooping bypass option-82-check {enable disable}	removed
ip helper dhcp-snooping vlan vlan_id [mac-address verification {enable disable}] [option-82 data-insertion {enable disable}]	removed
no ip helper dhcp-snooping vlan vlan_id	removed
ip helper dhcp-snooping port slot1/port1[-port1a] {block client-only trust}	removed
ip helper dhcp-snooping linkagg num {block client-only trust}	removed
ip helper dhcp-snooping port slot1/port1[-port1a] traffic-suppression {enable disable}	removed
ip helper dhcp-snooping port slot1/port1[-port1a] ip-source-filtering {enable disable}	removed
ip helper dhcp-snooping port binding {[enable disable] [mac_address port slot/port address ip_address vlan vlan_id]}	removed
no ip helper dhcp-snooping port binding mac_address port slot/port address ip_address vlan vlan_id	removed
ip helper dhcp-snooping port binding timeout seconds	removed
ip helper dhcp-snooping port binding action {purge renew}	removed
ip helper dhcp-snooping binding persistency {enable disable}	removed
ip udp relay {bootp nbdd nbnsnbdd dns tacacs tftp ntp port [name]}	ip udp relay service {tftp tacacs ntp nbns nbdd dns} [description <desc>]
n/a	ip udp relay port <port> [description <desc>]
no ip udp relay {bootp nbdd nbnsnbdd dns tacacs tftp ntp port}	ip udp relay no service {tftp tacacs ntp nbns nbdd dns}
n/a	ip udp relay no port <port>
ip udp relay {bootp nbdd nbnsnbdd dns tacacs tftp ntp port} vlan vlan_id	ip udp relay service {tftp tacacs ntp nbns nbdd dns} [description <desc>] vlan <vlan1[-vlan2]>

AOS Release 6	AOS Release 7
n/a	ip udp relay port <port> [description <desc>] vlan <vlan1[-vlan2]>
no ip udp relay {bootp nbdd nbnsnbdd dns tacacs tftp ntp port} vlan vlan_id	ip udp relay service {tftp tacacs ntp nbns nbdd dns} no vlan <vlan1[-vlan2]>
n/a	ip udp relay port <port> no vlan <vlan1[-vlan2]>
n/a	ip udp relay no statistics
ip helper no stats	no ip helper statistics
show ip helper dhcp-snooping vlan	removed
show ip helper dhcp-snooping port	removed
show ip helper dhcp-snooping binding	removed
show ip udp relay service [bootp nbdd nbnsnbdd dns tacacs tftp ntp port]	show ip udp relay service {tftp tacacs ntp nbns nbdd dns}
show ip udp relay [bootp nbdd nbnsnbdd dns tacacs tftp ntp port]	show ip udp relay port <port>
show ip udp relay destination [bootp nbdd nbnsnbdd dns tacacs tftp ntp port]	show ip udp relay
show ip udp relay statistics	show ip udp relay statistics service {tftp tacacs ntp nbns nbdd dns}
show ip udp relay statistics [bootp nbdd nbnsnbdd dns tacacs tftp ntp port]	show ip udp relay statistics port <port>
n/a	show ip udp relay statistics

DVMRP Commands

AOS Release 6	AOS Release 7
ip dvmrp status {enable disable}	ip dvmrp admin-state {enable disable}
ip dvmrp tunnel {local_name} {remote_address}	removed
no ip dvmrp tunnel {local_name} {remote_address}	removed
ip dvmrp tunnel {interface_name remote_address} ttl value	removed

ERP Commands

AOS Release 6	AOS Release 7
n/a	erp-ring <ring_id> {port <slot/port> linkagg <id>} virtual-sf-monitor {enable disable}

Ethernet Port Commands

AOS Release 6	AOS Release 7
interfaces {<slot> <slot/port[-port2]>} {admin autoneg } {enable disable}	interfaces {<slot> <slot/port[-port2]>} {admin-state autoneg } {enable disable}
trap slot[/port[-port2]] port link {enable disable on off}	interfaces {<slot> <slot/port1[-port2]>} link-trap {enable disable}
interfaces slot[/port[-port2]] speed {auto 10 100 1000 10000 max {100 1000}}	interfaces {<slot> <slot/port1[-port2]>} speed {10 100 1000 auto max {100 1000}}
n/a	interfaces {<slot> <slot/port1[-port2]>} flood-limit {bcast mcast ucast all} rate { pps <num> mbps <num> cap% <num> enable disable}
interfaces {<slot> <slot/port[-port2]>} no 12 statistics [cli]	clear interfaces {<slot> <slot/port1[-port2]>} 12-statistics [cli]
interfaces {<slot> <slot/port[-port2]>} port {<string> <num>}	interfaces {<slot> <slot/port1[-port2]>} alias {<string> <num>}
interfaces transceiver ddm [trap] {enable disable}	interfaces ddm[-trap] {enable disable}
n/a	interfaces {<slot> <slot/port1[-port2]>} ingress-bandwidth {mbps <num> [burst <mbits>] enable disable}
show interfaces [<slot> <slot/port[-port2]>] {status capability flood rate port accounting counters traffic pause}	show interfaces [<slot> <slot/port1[-port2]>] {status capability flood-rate port accounting counters [errors] traffic}
n/a	show interfaces [<slot> <slot/port1[-port2]>] ingress-rate-limit
show interfaces transceiver [<slot> <slot/port[-port2]>] transceiver [ddm w-low w-high a-low a-high actual]	show interfaces [<slot> <slot/port1[-port2]>] ddm [w-low w-high a-high a-low actual status]
show interfaces [<slot> <slot/port[-port2]>] port	show interfaces [<slot> <slot/port[-port2]>] alias
interfaces slot[/port[-port2]] hybrid	removed
show interfaces [slot[/port[-port2]]] hybrid	removed
interfaces {<slot> <slot/port[-port2]>} {ifg <num> flow {enable disable} clear-violation-all runt <num> runtsize <num> register {lwm dyncell} regval <num> pause}	removed
interfaces [no] e2e-flow-vlan	removed
interfaces cli-prompt {enable disable}	removed
10gig slot <slot> {phys-a phys-b}	removed
show interfaces [<slot> <slot/port[-port2]>] {e2e-flow-vlan flow collisions ifg register {lwm dyncell}}	removed
show 10gig [slot <slot>]	removed

Health Monitor Commands

AOS Release 6	AOS Release 7
health threshold temperature degrees	removed
health statistics reset	removed
show health threshold [rx txrx memory cpu temperature]	show health configuration
show health interval	show health configuration
show health [statistics]	show health
show health {slot/port} [statistics]	show health {port <slot/port> slot <slot>} [statistics]
show health all {memory cpu rx txrx}	show health all {memory cpu rx txrx}
show health slice slot	removed
show health fabric slot1[-slot2]	removed

HTTP Commands

AOS Release 6	AOS Release 7
[no] { http https } server	webview server { enable disable }
n/a	webview access { enable disable }
[no] { http https } ssl	webview force-ssl { enable disable }
{ http https } port { default <port> }	webview http-port { default <port> }
n/a	webview https-port { default <port> }
show http	show webview

IPsec Commands

AOS Release 6	AOS Release 7
no change	no change

IPv4 Commands

AOS Release 6	AOS Release 7
ip interface name admin {enable disable}	ip interface <name> admin-state {<enable> <disable>}
ip static-route ip_address [mask mask] gateway gateway [metric metric]	ip static-route ip_address [mask mask] {gateway gateway follows ip_address} [metric metric]
no ip static-route ip_address [mask mask] gateway ip_address [metric metric]	no ip static-route ip_address [mask mask] {gateway ip_address follows ip_address} [metric metric]

AOS Release 6	AOS Release 7
no ip service {all service_name port service_port}	removed
n/a	ip service {ftp ssh telnet} port {default <port>}
n/a	[no] ip service access [<ip_interface_name>]
arp ip_address hardware_address [alias] [arp-name] [<slot/port>]	arp <ip_address> <hardware_address> [alias] [<arp-name>] [port <slot/port>] [linkagg <agg_num>]
n/a	show ip router-id

IPv6 Commands

AOS Release 6	AOS Release 7
ipv6 interface if_name [vlan vid tunnel {tid 6to4}] [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}	new options [no ra-min-interval] [ra-cli-skew]
ipv6 interface if_name {enable disable}	ipv6 interface <if_name> admin-state {enable disable}
ipv6 neighbor ipv6_address hardware_address {if_name} slot/port	ipv6 neighbor <ipv6_address> <hardware_address> <if_name> {port <slot/port> linkagg <agg_id>}
traceroute6 {ipv6_address hostname} [if_name] [max-hop hop_count] [wait-time time] [port port_number] [probe-count probe]	new options [size size_value] [host-names {yes no}]
show ipv6 hosts [substring]	removed
clear ipv6 pmtu table	removed
show ipv6 neighbors [ipv6_prefix/prefix_length if_name hw hardware_address static]	no change
show ipv6 tcp ports	removed
n/a	show ipv6 tcp connections
n/a	show ipv6 tcp listeners
clear ipv6 traffic	removed
ipv6 redistrib {local static rip ospf isis bgp} into {rip ospf isis bgp} route-map routemap-name [status {enable disable}]	ipv6 redistrib {local static rip ospf isis bgp} into {rip ospf isis bgp} route-map <routemap-name> [admin-state {enable disable}]
ipv6 rip status {enable disable}	ipv6 rip admin-state {enable disable}

Link Aggregation Commands

AOS Release 6	AOS Release 7
static linkagg agg_num size size [name name] [admin state {enable disable}]	linkagg static agg <agg_num1[-agg_num2]> size size [name name] [admin-state {enable disable}] [multi-chassis active]
no static linkagg agg_num	no linkagg static agg <agg_num1[-agg_num2]>
static linkagg agg_num name name	linkagg static agg <agg_num1[-agg_num2]> name name
static linkagg agg_num no name	no linkagg static agg <agg_num1[-agg_num2]> name
static linkagg agg_num admin state {enable disable}	linkagg static agg <agg_num1[-agg_num2]> admin-state {enable disable}
static agg slot/port agg num agg_num	linkagg static port <slot/port1[-port2]> agg agg_num
static agg no slot/port	no linkagg static port <slot/port1[-port2]>
lacp linkagg agg_num size size	linkagg lacp agg <agg_num1[-agg_num2]> size size
no lacp linkagg agg_num	no linkagg lacp agg <agg_num1[-agg_num2]>
lacp linkagg agg_num name name	linkagg lacp agg <agg_num1[-agg_num2]> name name
lacp linkagg agg_num no name	no linkagg lacp agg <agg_num1[-agg_num2]> name
lacp linkagg agg_num admin state {enable disable}	linkagg lacp agg <agg_num1[-agg_num2]> admin- state {enable disable}
lacp linkagg agg_num actor admin key actor_admin_key	linkagg lacp agg <agg_num1[-agg_num2]> actor admin-key actor_admin_key
lacp linkagg agg_num no actor admin key	no linkagg lacp agg <agg_num1[-agg_num2]> actor admin-key
lacp linkagg agg_num actor system priority actor_system_priority	linkagg lacp agg <agg_num1[-agg_num2]> actor system-priority actor_system_priority
lacp linkagg agg_num no actor system priority	no linkagg lacp agg <agg_num1[-agg_num2]> actor system-priority
lacp linkagg agg_num actor system id actor_system_id	linkagg lacp agg <agg_num1[-agg_num2]> actor system-id actor_system_id
lacp linkagg agg_num no actor system id	no linkagg lacp agg <agg_num1[-agg_num2]> actor system-id
lacp linkagg agg_num partner system id partner_system_id	linkagg lacp agg <agg_num1[-agg_num2]> partner system-id partner_system_id
lacp linkagg agg_num no partner system id	no linkagg lacp agg <agg_num1[-agg_num2]> partner system-id
lacp linkagg agg_num partner system priority partner_system_priority	linkagg lacp agg <agg_num1[-agg_num2]> partner system-priority partner_system_priority

AOS Release 6	AOS Release 7
lACP linkagg agg_num no partner system priority	no linkagg lACP agg <agg_num1[-agg_num2]> partner system-priority
lACP linkagg agg_num partner admin key partner_admin_key	linkagg lACP agg <agg_num1[-agg_num2]> partner admin-key partner_admin_key
lACP linkagg agg_num no partner admin key	no linkagg lACP agg <agg_num1[-agg_num2]> partner admin-key
lACP agg slot/port actor admin key actor_admin_key	linkagg lACP port <slot/port1[-port2]> actor admin-key actor_admin_key
lACP agg no slot/port	no linkagg lACP port <slot/port1[-port2]>
lACP agg slot/port actor admin state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] none }	linkagg lACP port <slot/port1[-port2]> actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] none }
lACP agg slot/port actor admin state {[no] active} [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] none }	no linkagg lACP port <slot/port1[-port2]> actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] none }
lACP agg slot/port actor system id actor_system_id	linkagg lACP port <slot/port1[-port2]> actor system-id actor_system_id
lACP agg slot/port no actor system id	no linkagg lACP port <slot/port1[-port2]> actor system-id
lACP agg slot/port actor system priority actor_system_priority	linkagg lACP port <slot/port1[-port2]> actor system-priority actor_system_priority
lACP agg slot/port no actor system priority	no linkagg lACP port <slot/port1[-port2]> actor system-priority
lACP agg slot/port partner admin state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] none }	linkagg lACP port <slot/port1[-port2]> partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] none }
lACP agg slot/port partner admin state {[no] active} [[no] timeout] [[no] aggregate] [[no] synchronize] [[no] collect] [[no] distribute] [[no] default] [[no] expire] none }	no linkagg lACP port <slot/port1[-port2]> partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] none }
lACP agg slot/port partner admin system id partner_admin_system_id	linkagg lACP port <slot/port1[-port2]> partner admin-system-id partner_admin_system_id
lACP agg slot/port no partner admin system id	no linkagg lACP port <slot/port1[-port2]> partner admin-system-id
lACP agg slot/port partner admin key partner_admin_key	linkagg lACP port <slot/port1[-port2]> partner admin-key partner_admin_key
lACP agg slot/port no partner admin key	no linkagg lACP port <slot/port1[-port2]> partner admin-key
lACP agg slot/port partner admin system priority partner_admin_system_priority	linkagg lACP port <slot/port1[-port2]> partner admin-system-priority partner_admin_system_priority

AOS Release 6	AOS Release 7
lacp agg slot/port no partner admin system priority	no linkagg lacp port <slot/port1[-port2]> partner admin-system-priority
lacp agg slot/port actor port priority actor_port_priority	linkagg lacp port <slot/port1[-port2]> actor port-priority actor_port_priority
lacp agg slot/port no actor port priority	no linkagg lacp port <slot/port1[-port2]> actor port-priority
lacp agg slot/port partner admin port partner_admin_port	linkagg lacp port <slot/port1[-port2]> partner admin-port partner_admin_port
lacp agg slot/port no partner admin port	no linkagg lacp port <slot/port1[-port2]> partner admin-port
lacp agg slot/port partner admin port priority partner_admin_port_priority	linkagg lacp port <slot/port1[-port2]> partner admin-port-priority partner_admin_port_priority
lacp agg slot/port no partner admin port priority	no linkagg lacp port <slot/port1[-port2]> partner admin-port-priority
show linkagg [<agg_num>]	show linkagg agg [<agg_num1[-agg_num2]>]
show linkagg [agg_num] port [slot/port]	show linkagg agg [<agg_num1[-agg_num2]>] port [slot/port]

802.1AB Commands

AOS Release 6	AOS Release 7
lldp {slot/port slot chassis} lldpdu {tx rx tx-and-rx disable}	lldp {port <slot/port[-port]> slot <slot> chassis} lldpdu {tx rx tx-and-rx disable}
lldp {slot/port slot chassis} notification {enable disable}	lldp {port <slot/port[-port]> slot <slot> chassis} notification {enable disable}
lldp {slot/port slot chassis} tlv management {port-description system-name systemdescription system-capabilities management-address} {enable disable}	lldp {port <slot/port[-port]> slot <slot> chassis} tlv management {port-description system-name systemdescription system-capabilities management-address} {enable disable}
lldp {slot/port slot chassis} tlv dot1 {port-vlan vlan-name} {enable disable}	lldp {port <slot/port[-port]> slot <slot> chassis} tlv dot1 {port-vlan vlan-name} {enable disable}
lldp {slot/port slot chassis} tlv dot3 mac-phy {enable disable}	lldp {port <slot/port[-port]> slot <slot> chassis} tlv dot3 mac-phy {enable disable}
lldp {slot/port slot chassis} tlv med {power capability} {enable disable}	lldp {port <slot/port[-port]> slot <slot> chassis} tlv med {power capability} {enable disable}
show lldp [slot/port] statistics	show lldp [port <slot/port[-port]>] statistics
show lldp [slot/port slot] local-port	show lldp [port <slot/port[-port]> slot <slot>] local-port
show lldp [slot/port slot] remote-system	show lldp [port <slot/port[-port]> slot <slot>] remote-system
show lldp [slot/port slot] remote-system [med {network-policy inventory}]	show lldp [port <slot/port[-port]> slot <slot>] remote-system [med {network-policy inventory}]

AOS Release 6	AOS Release 7
show lldp [<slot slot/port>] config	show lldp [port <slot/port[-port]> slot <slot>] config
show lldp [<slot slot/port>] statistics	show lldp [port <slot/port[-port]> slot <slot>] statistics

Multicast Routing Commands

AOS Release 6	AOS Release 7
no change	no change

Network Time Protocol Commands

AOS Release 6	AOS Release 7
no change	no change

OSPF Commands

AOS Release 6	AOS Release 7
ip ospf status {enable disable}	ip ospf admin-state {enable disable}
ip ospf interface {interface_name} status {enable disable}	ip ospf interface {<interface_name>} admin-state {enable disable}
ip ospf restart-helper [status {enable disable}]	ip ospf restart-helper [admin-state {enable disable}]
ip ospf restart-helper strict-lsa-checking status {enable disable}	ip ospf restart-helper strict-lsa-checking admin-state {enable disable}

OSPFv3 Commands

AOS Release 6	AOS Release 7
ipv6 ospf status {enable disable}	ipv6 ospf admin-state {enable disable}
ipv6 ospf interface interface_name status {enable disable}	ipv6 ospf interface interface_name admin-state {enable disable}

PIM Commands

AOS Release 6	AOS Release 7
ip pim sparse status {enable disable}	ip pim sparse admin-state {enable disable}
ip pim dense status {enable disable}	ip pim dense admin-state {enable disable}
ip pim spt status {enable disable}	ip pim spt admin-state {enable disable}

AOS Release 6	AOS Release 7
ipv6 pim sparse status {enable disable}	ipv6 pim sparse admin-state {enable disable}
ipv6 pim dense status {enable disable}	ipv6 pim dense admin-state {enable disable}
ipv6 pim spt status {enable disable}	ipv6 pim spt admin-state {enable disable}

Port Security Commands

AOS Release 6	AOS Release 7
port-security {slot/port[-port2] chassis} [enable disable]	port-security {port <slot/port[-port2]> chassis} [learning-enable learning-disable]
no port security slot/port[-port2]	no port security {port <slot/port[-port2]>}
port-security shutdown minutes [convert-to-static {enable disable}]	port-security learning-window <minutes> [convert-to-static {enable disable}]
port-security shutdown 0	no port-security learning-window
port-security slot/port[-port2] maximum number	port-security port <slot/port[-port2]> maximum <number>
port-security slot/port[-port2] max-filtering number	port-security port <slot/port[-port2]> max-filtering <number>
port-security {slot/port[-port2] chassis} convert-to-static	port-security {port <slot/port[-port2]> chassis} convert-to-static
port-security slot/port mac mac_address [vlan vlan_id]	removed
port-security slot/port no mac {all mac_address} [vlan vlan_id]	removed
port-security slot/port[-port2] mac-range [low mac_address high mac_address low mac_address high mac_address]	port-security port <slot/port[-port2]> mac-range [low mac_address high mac_address low mac_address high mac_address]
port-security slot/port[-port2] violation {restrict shutdown}	port-security port <slot/port[-port2]> violation {restrict shutdown}
port-security slot/port release	removed
port-security slot/port[-port2] learn-trap-threshold <number>	port-security port <slot/port[-port2]> learn-trap-threshold <number>
show port-security [slot/port[-port2] slot]	show port-security [port <slot/port[-port2]> slot <slot>]
show port-security shutdown	show port-security learning-window

Policy Server Commands

AOS Release 6	AOS Release 7
policy server ip_address admin {up down}	policy server ip_address admin-state {enable disable}

Port Manager Commands

AOS Release 6	AOS Release 7
n/a	show violation [port <slot/port[-port]> linkagg <aggnum[-aggnum]>]
n/a	clear violation {port <slot/port[-port]> linkagg <aggnum[-aggnum]>}

Port Mapping Commands

AOS Release 6	AOS Release 7
port mapping <id> [no user-port {<slot/port[-port]> linkagg <agg_id> slot <slot_id>} [no network-port {<slot/port[-port]> linkagg <agg_id> slot <slot_id>}]	no port-mapping <id> [user-port {<slot/port[-port]> linkagg <agg_id> slot <slot_id>} [network-port {<slot/port[-port]> linkagg <agg_id> slot <slot_id>}]

Port Mirroring and Monitoring Commands

AOS Release 6	AOS Release 7
port mirroring port_mirror_sessionid [no] source slot/port[-port2] [slot/port[-port2]...] destination slot/port [rpmir-vlan vlan_id] [bidirectional inport outport] [unblocked vlan_id] [enable disable]	port-mirroring <port_mirror_sessionid> [no] source {policy <slot/port[-port2] [slot/port[-port2]...]>} destination <slot/port> [rpmir-vlan <vlan_id>] [bidirectional inport outport] [unblocked-vlan <vlan_id>] [enable disable]
port monitoring port_monitor_sessionid source slot/port [{no file file filename [size filesize] [overwrite {on off}]]} [inport outport bidirectional] [timeout seconds] [enable disable]	port-monitoring <port_monitor_sessionid> source <slot/port> [{no file file <filename> [size <filesize>] [overwrite {on off}]]} [inport outport bidirectional] [timeout <seconds>] [enable disable] [capture-type {full brief}]

QoS Commands

AOS Release 6	AOS Release 7
qos default servicing mode {strict-priority wrr [w0 w1 w2 w3 w4 w5 w6 w7] priority-wrr [w0 w1 w2 w3 w4 w5 w6 w7] drr [w0 w1 w2 w3 w4 w5 w6 w7]}	removed
qos [no] classifyl3 bridged	removed
qos [no] classify fragments	removed
qos default bridged disposition {accept deny drop}	removed
qos default routed disposition {accept deny drop}	removed
qos default multicast disposition {accept deny drop}	removed
qos nms priority	removed
qos no nms priority	removed
qos flow timeout	removed
qos fragment timeout	removed
qos port slot/port servicing mode {strict-priority wrr [w0 w1 w2 w3 w4 w5 w6 w7] prioritywrr [w0 w1 w2 w3 w4 w5 w6 w7] drr [w0 w1 w2 w3 w4 w5 w6 w7] default}	removed
qos port slot/port qn {minbw maxbw} kbps	removed
qos port slot/port no qn {minbw maxbw} kbps	removed
qos port slot/port maximum bandwidth bps	removed
qos port slot/port no maximum bandwidth	removed
qos port slot/port maximum default buffers <buf>	qos port slot/port maximum depth <val>
qos port slot/port no maximum default depth	qos port slot/port no maximum depth
qos port slot/port maximum default buffers <buf>	removed
qos port slot/port no maximum default buffers	removed
show qos queue	removed
show qos classify	removed
policy import <string>	removed
policy rule rule_name [enable disable] [from {ldap cli}] [precedence precedence] [condition condition] [action action] [validity period name no validity period] [save] [log [log-interval seconds]] [count {packets bytes}] [trap no trap] [default-list no default-list]	policy rule <rule_name> [enable disable] [from {ldap cli}] [precedence <precedence>] [condition <condition>] [action <action>] [validity-period <name> no validity-period] [save] [log [log-interval <seconds>]] [count {packets bytes}] [trap no-trap] [default-list]
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]	policy validity-period <name> [from {ldap cli} days <days> months <months> hours <hh:mm> to <hh:mm>] [interval <mm:dd:yyyy> <hh:mm> to <mm:dd:yyyy> <hh:mm>]

AOS Release 6	AOS Release 7
policy validity-period <name> no {hours interval days <days> months <months>}	policy validity-period <name> no {hours interval days <days> months <months>}
policy condition condition_name source interface type [ethernet wan ethernet-10 ethernet-100 ethernet-1G ethernet-10G]	removed
policy condition condition_name no source interface type	removed
policy condition condition_name destination interface type [ethernet wan ethernet-10 ethernet-100 ethernet-1G ethernet-10G]	removed
policy condition condition_name no destination interface type	removed
n/a	policy condition <condition_name> [no] fragments
policy action action_name minimum bandwidth bps	removed
policy action action_name no minimum bandwidth	removed
policy action action_name maximum buffers val	removed
policy action action_name no maximum buffers	removed
policy action action_name minimum depth bytes	removed
policy action action_name no minimum depth	removed
policy action action_name alternate gateway ip ip_address	removed
policy action action_name no alternate gateway ip	removed
n/a	policy action <action_name> {pir <rate> pbs <size> cir <rate> cbs <size> cpu-priority <0-7>}
show policy classify {12 13 multicast} [applied] source interface type {ethernet wan ethernet-10 ethernet-100 ethernet-1G ethernet-10G}	removed
show policy classify {12 13 multicast} [applied] destination interface type {ethernet wan ethernet-10 ethernet-100 ethernet-1G ethernet-10G}	removed

RIP Commands

AOS Release 6	AOS Release 7
ip rip interface {interface_name} status {enable disable}	ip rip interface {interface_name} admin-state {enable disable}

Sflow Commands

AOS Release 6	AOS Release 7
sflow receiver <num> [name <string> timeout {<seconds> forever} address {<ip_address> <ipv6address>} udp-port <port> packet-size <size> Version <num>]	sflow receiver <receiver_index> {name <string> timeout {<seconds> forever} address {<ip_address> <ipv6address>} udp-port <port> packet-size <size> Version <num> release}
sflow receiver <receiver_index> [release]	sflow receiver <receiver_index> {name <string> timeout {<seconds> forever} address {<ip_address> <ipv6address>} udp-port <port> packet-size <size> Version <num> release}
sflow sampler <num> <portlist> [receiver <receiver_index> rate <value> sample-hdr-size <size>]	sflow sampler <num> port <slot/port[-port]> {receiver <receiver_index> rate <value> sample-hdr-size <size>}
sflow poller <num> <portlist> [receiver <receiver_index> interval <value>]	sflow poller <num> port <slot/port[-port]> {receiver <receiver_index> interval <value>}

SLB Commands

AOS Release 6	AOS Release 7
ip slb admin {enable disable}	ip slb admin-state {enable disable}
ip slb server ip ip_address cluster cluster_name [admin status {enable disable}]	ip slb server ip <ip_address> cluster <cluster_name> [admin-state {enable disable}]

SNMP Commands

AOS Release 6	AOS Release 7
snmp community map <map> user <user>	snmp community-map <map> user <user_name>
snmp community map <map> user <user> {enable disable}	snmp community-map <map> user <user_name> {enable disable}
no snmp community map <string>	no snmp community-map <map>
show snmp community map	show snmp community-map
show snmp trap filter	show snmp-trap filter-ip
show snmp trap replay	show snmp-trap replay-ip
show snmp trap config	show snmp-trap config
snmp trap absorption {enable disable}	snmp-trap absorption {enable disable}
snmp trap to webview {enable disable}	snmp-trap to-webview {enable disable}

Source Learning Commands

AOS Release 6	AOS Release 7
mac-address-table [permanent] mac_address {slot/port linkagg link_agg} vid [bridging filtering]	mac-learning vlan <vid> {port <slot/port> linkagg <link_agg>} static mac-address <mac_address> [bridging filtering]
no mac-address-table [permanent learned] [mac_address {slot/port linkagg link_agg} vid]	no mac-learning [vlan <vid>] [port <slot/port> linkagg <link_agg>] {static dynamic} [mac-address <mac_address>]
mac-address-table static-multicast multicast_address {slot1/port1[-port1a][slot2/port2[linkagg link_agg]} vid	mac-learning vlan <vid> {port <slot1/port1[-port1]> <[slot2/port2]> linkagg <link_agg>} multicast mac-address <multicast_address> [group <groupid>]
no mac-address-table static-multicast [<mac_address> {slot1/port1[-port1a][slot2/port2[linkagg link_agg]} vid]	no mac-learning [vlan <vid>] [port <slot1/port1[-port1]> <[slot2/port2]> linkagg <link_agg>] {multicast } [mac-address <multicast_address>]
source-learning {port <slot/port> linkagg <agg_num>} enable disable	mac-learning {port <slot/port> linkagg <link_agg>} {enable disable}
show source-learning [port slot/port linkagg link_agg]	show mac-learning learning-state [slot <slot> port <slot/port> linkagg <link_agg>]
show mac-address-table [permanent learned quarantined] [mac_address] [slot slot slot/port] [linkagg link_agg][vid vid1-vid2]	show mac-learning [summary] [multicast static dynamic quarantined] [vlan <vid1[-vid2]>] [slot <slot> port <slot/port>] [linkagg <link_agg>] [mac-address <mac_address>]
source-learning chassis-distributed {enable disable}	mac-learning mode [centralized distributed]
show source-learning chassis-distributed	show mac-learning mode

STP Commands

AOS Release 6	AOS Release 7
bridge mode {flat 1x1}	spantree mode {flat per-vlan}
bridge protocol {stp rstp mstp}	spantree protocol {stp rstp mstp}
bridge <instance> protocol {stp rstp mstp}	removed
bridge cist protocol {stp rstp mstp}	spantree cist protocol {stp rstp mstp}
bridge 1x1 <vid> protocol {stp rstp}	spantree vlan <vid> protocol {stp rstp}
bridge mst <msti_id> region name <name>	spantree mst <msti_id> region name <name>
bridge mst <msti_id> region no name	no spantree mst <msti_id> region name
bridge mst <msti_id> region revision level <rev_level>	spantree mst <msti_id> region revision-level <rev_level>
bridge mst <msti_id> region max hops <max_hops>	spantree mst <msti_id> region max-hops <max_hops>
bridge msti <msti_id> [name <name>]	spantree msti <msti_id> msti_id [name <name>]

AOS Release 6	AOS Release 7
bridge no msti <msti_id>	no spantree msti <msti_id>
bridge msti <msti_id> no name	no spantree msti <msti_id> name
bridge msti <msti_id> vlan <vid_range>	spantree msti <msti_id> vlan <vid_range>
bridge msti <msti_id> no vlan <vid_range>	no spantree msti <msti_id> vlan <vid_range>
bridge priority <priority>	spantree priority <priority>
bridge <instance> priority <priority>	removed
bridge cist priority <priority>	spantree cist priority <priority>
bridge msti <msti_id> priority <priority>	spantree msti <msti_id> priority <priority>
bridge 1x1 <vid> priority <priority>	spantree vlan <vid> priority <priority>
bridge hello time <seconds>	spantree hello-time <seconds>
bridge <instance> hello time <seconds>	removed
bridge cist hello time <seconds>	spantree cist hello-time <seconds>
bridge 1x1 vid hello time <seconds>	spantree vlan <vid> hello-time <seconds>
bridge max age <seconds>	spantree max-age <seconds>
bridge <instance> max age <seconds>	removed
bridge cist max age <seconds>	spantree cist max-age <seconds>
bridge 1x1 <vid> max age <seconds>	spantree vlan <vid> max-age <seconds>
bridge forward delay <seconds>	spantree forward-delay <seconds>
bridge <instance> forward delay <seconds>	removed
bridge cist forward delay <seconds>	spantree cist forward-delay <seconds>
bridge 1x1 <vid> forward delay <seconds>	spantree vlan <vid> forward-delay <seconds>
bridge bpdu-switching {enable disable}	spantree bpdu-switching {enable disable}
bridge <instance> bpdu-switching {enable disable}	removed
bridge cist bpdu-switching {enable disable}	spantree cist bpdu-switching {enable disable}
bridge 1x1 <vid> bpdu-switching {enable disable}	spantree vlan <vid> bpdu-switching {enable disable}
bridge path cost mode {auto 32bit}	spantree path-cost-mode {auto 32bit}
bridge [msti <msti_id>] auto-vlan-containment {enable disable}	spantree [msti <msti_id>] auto-vlan-containment {enable disable}
bridge instance {slot/port logical_port} {enable disable}	removed
bridge cist {slot/port logical_port} {enable disable}	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} {enable disable}
bridge 1x1 <vid> {slot/port logical_port} {enable disable}	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} {enable disable}
bridge instance {slot/port logical_port} priority priority	removed

AOS Release 6	AOS Release 7
bridge cist {slot/port logical_port} priority priority	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} priority priority
bridge msti <msti_id> {slot/port logical_port} priority priority	spantree msti <msti_id> {port <slot/port> linkagg <linkagg1[-linkagg2]>} priority priority
bridge 1x1 <vid> {slot/port logical_port} priority priority	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} priority priority
bridge instance {slot/port logical_port} path cost path_cost	removed
bridge cist {slot/port logical_port} path cost path_cost	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} path-cost path_cost
bridge msti <msti_id> {slot/port logical_port} path cost path_cost	spantree msti <msti_id> {port <slot/port> linkagg <linkagg1[-linkagg2]>} path-cost path_cost
bridge 1x1 <vid> {slot/port logical_port} path cost path_cost	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} path-cost path_cost
bridge instance {slot/port logical_port} mode {forwarding blocking dynamic}	removed
bridge cist {slot/port logical_port} mode {dynamic blocking forwarding}	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} mode {dynamic blocking forwarding}
bridge 1x1 <vid> {slot/port logical_port} mode {dynamic blocking forwarding}	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} mode {dynamic blocking forwarding}
bridge instance {slot/port logical_port} connection {noptp ptp autoptp edgeport}	removed
bridge cist {slot/port logical_port} connection {noptp ptp autoptp edgeport}	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} connection {noptp ptp autoptp}
bridge 1x1 <vid> {slot/port logical_port} connection {noptp ptp autoptp edgeport}	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} connection {noptp ptp autoptp}
bridge cist {slot/port logical_port} admin-edge {on off enable disable}	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} admin-edge {enable disable}
bridge 1x1 <vid> {slot/port logical_port} admin-edge {on off enable disable}	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} admin-edge {enable disable}
bridge cist {slot/port logical_port} auto-edge {on off enable disable}	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} auto-edge {enable disable}
bridge 1x1 <vid> {slot/port logical_port} auto-edge {on off enable disable}	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} auto-edge {enable disable}

AOS Release 6	AOS Release 7
bridge cist {slot/port logical_port} {restricted-role root-guard} {on off enable disable}	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} {restricted-role root-guard} {enable disable}
bridge 1x1<vid> {slot/port logical_port} {restricted-role root-guard} {on off enable disable}	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} {restricted-role root-guard} {enable disable}
bridge cist {slot/port logical_port} restricted-tcn {on off enable disable}	spantree cist {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} restricted-tcn {enable disable}
bridge 1x1<vid> {slot/port logical_port} restricted-tcn {on off enable disable}	spantree vlan <vid> {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} restricted-tcn {enable disable}
bridge cist txholdcount value	spantree cist txholdcount value
bridge 1x1<vid> txholdcount {value}	spantree vlan <vid> txholdcount {value}
bridge port slot/port 10gig os8800optimized {enable disable}	removed
bridge rrstp	removed
no bridge rrstp	removed
bridge rrstp ring ring_id port1 {slot/port linkagg agg_num} port2 {slot/port linkagg agg_num} vlan-tag vlan_id [status {enable disable}]	removed
no bridge rrstp ring [ring_id]	removed
bridge rrstp ring ring_id vlan-tag vid	removed
bridge rrstp ring ring_id status {enable disable}	removed
show spantree <instance>	removed
show spantree 1x1 [vid]	show spantree [vlan <vid>]
show spantree <instance> ports [forwarding blocking active configured]	removed
show spantree 1x1 [vid] ports [forwarding blocking active configured]	show spantree [vlan <vid>] ports [forwarding blocking active configured]
show spantree mst port {slot/port logical_port}	show spantree mst {port <slot/port> linkagg <linkagg1[-linkagg2]>}
show bridge rrstp configuration	removed
show bridge rrstp ring [ring_id]	removed
show spantree map-msti	show spantree [vlan <vlan_id>] map-msti
bridge mode 1x1 pvst+ {enable disable}	spantree pvst+compatibility {enable disable}
bridge port {slot/port agg_num} pvst+ {auto enable disable}	spantree pvst+compatibility {port <slot/port> linkagg <linkagg1[-linkagg2]>} {enable disable auto}

System Services Command

AOS Release 6	AOS Release 7
update {miniboot uboot-miniboot}	removed
more [<string> size]	Replaced by linux version of command: more
no more	removed
show more	removed
ls [-r] [<string>]	Replaced by linux version of command: ls
rm [-r] [<string>]	Replaced by linux version of command: rm
cp [-r] [<string>]	Replaced by linux version of command: cp
fsck /flash [repair no-repair]	removed
newfs /flash	removed
dshell	removed
view <string>	removed
tftp {<string> <ip_address>} {get put} source-file <string> [ascii destination-file <string>]	removed
backup <string> <string>	removed
restore <string> [display-only <string>]	removed
freespace [/flash]	freespace [/flash /uflash]
n/a	usb {enable disable}
n/a	usb auto-copy {enable disable}
n/a	show usb statistics
no ktrace	removed
ssh6 <dest_address>	removed
sftp6 <dest_address>	removed
show ssh config	removed
show history	history
show swlog	show swlog [appid {<appname> all}]
show log swlog [timestamp <date> <time> session <int> appid <app> level <level>]	show log swlog
swlog clear	swlog clear [slot {<int> all}]
swlog output flash file-size integer	swlog output flash-file-size <size>
[no] swlog	swlog [appid {<appname> all} subapp {<0-31> all}] {enable disable}
swlog appid appidlist level level	swlog appid <name> subapp <0-31> level <num> [vrf <vrf>]
no swlog appid appidlist	removed
n/a	[no] swlog preamble

AOS Release 6	AOS Release 7
n/a	[no] swlog duplicate-detect
n/a	swlog hash-time-limit <limit>
n/a	swlog output tty {enable disable}
session banner {cli ftp http} <file_name >	session {cli ftp http} banner <file_name>
session banner no {cli ftp http}	no session {cli ftp http} banner
session timeout {cli http ftp} <minutes>	session {cli ftp http} timeout <minutes>
session {ftp tftp sftp telnet} port <port>	ip service {ftp ssh telnet} port {default <port>}
upgrade ni <int> license-key <"string">	removed
exit	Replaced by linux version of command: exit
kill <int>	Replaced by linux version of command: kill
alias <string> <string>	Replaced by linux version of command: alias
no alias [all <string>]	Replaced by linux version of command: unalias
show alias [all <string>]	Replaced by linux version of command: alias
cd [<directory>]	Replaced by linux version of command: cd
pwd	Replaced by linux version of command: pwd
mkdir [<directory>]	Replaced by linux version of command: mkdir
rmdir [<directory>]	Replaced by linux version of command: rmdir
dir [<directory>]	Replaced by linux version of command: ls
rename <file1> <file2>	Replaced by linux version of command: mv
delete <file>	Replaced by linux version of command: rm
mv <file1> <string>	Replaced by linux version of command: mv
move <file1> <string>	Replaced by linux version of command: mv
attrib {+w -w} <string>	removed: same command as chmod
ftp {<string> <ip_address>}	Replaced by linux version of command: ftp
vi <filename>	Replaced by linux version of command: vi
telnet {<string> <ip_address>}	Replaced by linux version of command: telnet
scp {<string> <ip_address>} {<string> <ip_address>}	Replaced by linux version of command: scp
aclman	removed
rz	removed
install {<string>}+	removed
scp-sftp {enable disable}	removed
ftp6 {<string> <ipv6_address>} <interface>	removed
telnet6 {<string> <ipv6_address>} <interface>	removed
prompt [none] [time system user date prefix string <string>]*	removed

VLAN Manager Commands

AOS Release 6	AOS Release 7
vlan <vid1[-vid2]> 802.1q {<slot/port1[-port2]> <aggregate_id>}	vlan <vid1[-vid2]> members {port <slot/port1[-port2]> linkagg <agg1[-agg2]>} tagged
no vlan <vid1[-vid2]> 802.1q {<slot/port[-port2]> <aggregate_id>}	no vlan <vid1[-vid2]> members {port <slot/port1[-port2]> linkagg <agg1[-agg2]>}
vlan <vid> port default {<slot/port> <link_agg>}	vlan <vid> members {port <slot/port1[-port2]> linkagg <agg1[-agg2]>} untagged
no vlan <vid1[-vid2]> port default {<slot/port> <link_agg>}	no vlan <vid1[-vid2]> members {port <slot/port1[-port2]> linkagg <agg1[-agg2]>}
vlan <vid1[-vid2]> [enable disable]	vlan <vid1[-vid2]> [admin-state {enable disable}]
no vlan vid mac mac_address	removed
no vlan vid mac range low_mac_address	removed
no vlan vid ip ip_address [subnet_mask]	removed
no vlan vid ipx ipx_net	removed
no vlan vid protocol {ip-e2 ip-snap ipx-e2 ipx-nov ipx-llc ipx-snap decnet appletalk ethertype type dsapssap dsap/ssap snap snaptype}	removed
no vlan vid port slot/port	removed
no vlan port mobile slot/port	removed
no vlan vid router ipx	removed
show vlan [<vid1[-vid2]>] [port [<slot/port> <link_agg>]]	show vlan [<vid1[-vid2]>] [members [port <slot/port1[-port2]> linkagg <agg1[-agg2]>]]
show vlan router mac-status	removed
vlan 802.1q slot/port frame type {all tagged}	removed
show 802.1q {slot/port aggregate_id}	removed
show vlan gvrp [vid1[-vid2]]	removed
show vlan ipmvlan [ipmvlan-id1[-ipmvlan-id2]]	removed
vlan vid1[-vid2] {1x1 flat} stp {enable disable}	removed
vlan <vid1[-vid2]> stp {enable disable}	spantree vlan <vid1[-vid2]> admin-state {enable disable}
vlan vid1[-vid2] mobile-tag {enable disable}	removed
vlan vid router ipx ipx_net [rip active inactive triggered] [e2 llc snap novell] [timeticks ticks]	removed

VLAN Stacking Commands

AOS Release 6	AOS Release 7
ethernet-service {svlan ipmvlan management-vlan} svid1[-svid2] [enable disable] [[1x1 flat] stp {enable disable}] [name description]	ethernet-service svlan <svlan1[-svlan2]> [admin-state {enable disable}] [stp {enable disable}] [name <description>]
no ethernet-service {svlan ipmvlan management-vlan} svid1[-svid2]	no ethernet-service svlan <svlan1[-svlan2]>
ethernet-service service-name service-name {svlan ipmvlan} svid	ethernet-service service-name <service-name> svlan <svlan>
no ethernet-service service-name service-name {svlan ipmvlan} svid	no ethernet-service service-name <service-name> svlan <svlan>
ethernet-service svlan svid1[-svid2] nni {slot/port1[-port2] linkagg agg_num} [stp erp]	ethernet-service svlan <svlan1[-svlan2]> nni {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>}
no ethernet-service svlan svid1[-svid2] nni {slot/port1[-port2] linkagg agg_num}	no ethernet-service svlan <svlan1[-svlan2]> nni {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>}
ethernet-service nni {slot/port1[-port2] agg_num} [tpid value] [{stp gvrp} legacy-bpdu {enable disable}] [transparent-bridging {enable disable}]	ethernet-service nni {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} [tpid <value>] [{stp mvrp} legacy-bpdu {enable disable}]
n/a	no ethernet-service nni {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>}
ethernet-service sap sapid uni {slot/port1[-port2] linkagg agg_num}	ethernet-service sap <sapid> uni {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>}
ethernet-service sap sapid no uni {slot/port1[-port2] linkagg agg_num}	no ethernet-service sap <sapid> uni {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>}
ethernet-service sap sapid no cvlan {all cvid cvid1-cvid2 untagged}	no ethernet-service sap <sapid> cvlan {all <cvlan1[-cvlan2]> untagged}
ethernet-service {svlan ipmvlan} svid1[-svid2] source-learning {enable disable}	ethernet-service svlan <svlan1[-svlan2]> source-learning {enable disable}
ethernet-service uni-profile uni-profile-name [l2-protocol {stp 802.1x 802.1ab 802.3ad gvrp amap} {peer discard tunnel}	ethernet-service uni-profile uni-profile-name [l2-protocol {stp 802.1x 802.1ab 802.3ad amap mvrp} {peer discard tunnel}
ethernet-service uni {slot/port1[-port2] agg_num} uni-profile uni-profile-name	ethernet-service uni {port <slot/port1[-port2]> linkagg <linkagg1[-linkagg2]>} uni-profile <uni-profile-name>
show ethernet-service mode	removed
show ethernet-services vlan [svid1-[svid2]]	show ethernet-services vlan [svid1-[svid2]]
show ethernet-services port {slot/port linkagg agg_num}	show ethernet-services {port <slot/port> linkagg <linkagg>}
show ethernet-services nni [slot/port linkagg agg_num]	show ethernet-services nni [port <slot/port> linkagg <linkagg>]

AOS Release 6	AOS Release 7
show ethernet-services uni [slot/port linkagg agg_num]	show ethernet-services uni [port <slot/port> link- agg <linkagg>]

VRRP Commands

AOS Release 6	AOS Release 7
no change	no change

OmniSwitch CLI Short Cuts

The following table provides a list of some of the CLI command short cuts (hot keys):

Delete Short Cuts	Description
Delete	Removes one character to the right of the cursor.
Backspace	Removes one character to the left of the cursor.
Ctrl-U	Erases a line.
Ctrl-W	Erases a word.
Ctrl-K	Delete end of line.
Ctrl-X Backspace	Delete beginning of line.
Alt-D	Delete end of word.
Alt-Backspace	Delete beginning of word.
Ctrl-Y	Paste previously deleted/memorized word.
Completion Short Cuts	Description
TAB	Finishes a partial command.
Alt-?	Shows how a partial command would be finished.
Alt-*	Finishes a partial command with every word possible.
Ctrl-X /	Shows completion using filenames only
Alt-/	Performs completion using filenames only
Cursor Short Cuts	Description
Ctrl-A	Moves the cursor to the beginning of the current line.
Ctrl-E	Moves the cursor to the end of the current line.
Ctrl-X Ctrl-X	Moves the cursor to the beginning/previous position in the current line.
Ctrl-] <char>	Moves the cursor to the next occurrence of <char>
Ctrl-Alt-] <char>	Moves the cursor to the previous occurrence of <char>
Alt-B	Moves the cursor to beginning of word.
Alt-F	Moves the cursor to end of word.
History Short Cuts	Description
Up Arrow	Allows user to scroll forward through former commands.
Down Arrow	Allows user to scroll backward through former commands.
Ctrl-R	Start/Resume backward history search mode.
Ctrl-S	Start/Resume forward history search mode.
Ctrl-J	Start editing history entry found in search mode.
Other Short Cuts	Description
Ctrl-R	Redisplays a line.
Ctrl-L	Clears screen.

Ctrl-T	Swaps two characters.
Alt-T	Swaps two words.
Alt-C	Switches character to upper case.
Alt-U	Switches end of word to upper case.
Alt-L	Switches end of word to lower case.
Ctrl- <u></u>	Undo (e.g. backspaces)
Alt-#	Comment out current line.
Alt-<number>	Repeat next command.

CLI Quick Reference

Ethernet Port Commands

```
interfaces {slot/ slot/port[-port2]} {admin-state | autoneg | epp} {enable|disable}
interfaces { slot / slot/port [-port2] } speed { 10 | 100 | 1000 | auto | max {10 | 100 | 1000}}
interfaces {slot/ slot/port[-port2]} crossover {auto | mdix | mdi}
interfaces {slot/ slot/port[-port2]} duplex {full | half | auto}
interfaces slot/port alias description
clear interfaces {slot / slot/port[-port2] } l2-statistics [cli]
interfaces {slot / slot/port[-port2] } max-frame-size bytes
interfaces {slot/ slot/port[-port2]} flood-limit {bcast|mcast|uucast|all} rate {pps pps_num|
    mbps mbps_num | cap% cap_num | enable | disable}
interfaces {slot/ slot/port[-port2]} ingress-bandwidth {mbps| enable | disable}
interfaces slot/port[-port2]] pause {rx | disable}
interfaces [slot / slot/port [-port2]] link-trap {enable|disable}
interfaces ddm {enable | disable}
interfaces ddm-trap {enable | disable}
clear violation {port slot/port[-port2] | linkagg agg_id[-agg_id2]}
show interfaces [slot / slot/port[-port2]]
show interfaces [slot / slot/port[-port2]] alias
show interfaces [slot / slot/port[-port2]] status
show interfaces [slot / slot/port[-port2]] capability
show interfaces [slot / slot/port[-port2]] accounting
show interfaces [slot / slot/port[-port2]] counters
show interfaces [slot / slot/port[-port2]] counters errors
show interfaces [slot / slot/port[-port2]] flood-rate
show interfaces [slot / slot/port[-port2]] traffic
show interfaces [slot/ slot/port[-port1]] ddm [W-LOW W-HIGH STATUS A-LOW A-HIGH
    ACTUAL]
show transceivers [slot slot]
show violation {port slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

UDLD Commands

```
udld {enable | disable}
udld port slot/port[-port2] {enable | disable}
udld port [slot/port[-port2]] mode {normal | aggressive}
udld port [slot/port[-port2]] probe-timer seconds
no udld port [slot/port[-port2]] probe-timer
udld port [slot/port[-port2]] echo-wait-timer seconds
no udld port [slot/port[-port2]] echo-wait-timer
clear udld statistics [port slot/port]
```

```
show udld configuration
show udld configuration port [slot/port]
show udld statistics port slot/port
show udld neighbor port slot/port
show udld status port [slot/port]
```

Source Learning Commands

```
mac-learning {port slot/port | linkagg linkagg} {enable | disable}
mac-learning flush {dynamic | static | multicast} [mac-address mac_address]
mac-learning flush domain {all | vlan {vlan vlan_id [port slot/port | linkagg agg_id ]} | spb
    {serviceid service_id | sap slot/port:encap | mesh-sdp mesh_id | isid instance_id} | evb
    {serviceid service_id}} {dynamic | static | static-multicast} [mac-address mac_address]
mac-learning {vlan vlan_id {port slot/port / linkagg linkagg_id}} static mac-address
    mac_address [bridging | filtering]
mac-learning flush [vlan vlan_id [port slot/port / linkagg linkagg_id]] static [mac-address
    mac_address]
mac-learning {vlan vlan_id {port slot/port | linkagg linkagg_id}} multicast mac-address
    multicast_address [group group_id]
mac-learning flush [vlan vlan_id [port slot/port | linkagg linkagg_id]] multicast [mac-address
    multicast_address]
mac-learning aging-time {seconds | default}
no mac-learning aging-time
mac-learning mode [centralized | distributed]
show mac-learning [summary] [multicast | static | dynamic] [vlan vlan_id [-vlan_id2]] [slot
    slot | port slot/port] [linkagg agg_id] [mac-address mac_address]
show mac-learning [summary | multicast | static | dynamic] [vlan vlan_id [-vlan_id2]] {remote
    [mac_address]}
show mac-learning aging-time
show mac-learning learning-state [vlan vlan[-vlan2] / port slot/port | linkagg linkagg]
show mac-learning mode
mac-ping dst-mac mac vlan vlan-id [priority vlan-priority] [drop-eligible {true | false}]
    [count count] [interval delay] [size size] [isid-check isid]
```

VLAN Management Commands

```
vlan vlan_id [admin-state {enable | disable}] [name description]
no vlan vlan_id
vlan vlan_id [-vlan_id2] members {port slot/port[-port1] | linkagg linkagg_id[-linkagg_id2]}
    untagged
no vlan vlan_id [-vlan_id2] members {port slot/port[-port1] | linkagg_id linkagg_id[-
    linkagg_id2]}
vlan vlan_id[-vlan_id2] members {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]}
    tagged
```

```

no vlan vlan_id[-vlan_id2] members {port slot/port[-port2] | linkagg linkagg_id[-
linkagg_id2]}
vlan vlan_id mtu-ip size
show vlan [vlan_id]
show vlan [vlan_id [-vlan_id2]] members [port [slot/port[-port2]/ linkagg linkagg_id [-
linkagg_id2]]]

```

High Availability VLAN Commands

```

server-cluster cluster-id [name cluster-name] [mode {L2 | L3}] [admin-state
{enable|disable}]
no server-cluster cluster-id
server-cluster cluster-id vlan vlan_id
server-cluster cluster-id mac-address mac-address
server-cluster cluster-id ip ip-address [ mac-address {static mac-address | dynamic}]
server-cluster cluster-id igmp-mode {enable | disable}
server-cluster cluster-id ip-multicast ipm-address
server-cluster cluster-id port {slot/port[-port2] | all}
no server-cluster cluster-id port {slot/port[-port2] | all}
server-cluster cluster-id linkagg agg_id[-agg_id2]
no server-cluster cluster-id linkagg agg_id[-agg_id2]
show server-cluster [cluster-id port]

```

Distributed Spanning Tree Commands

```

spantree mode {flat | per-vlan}
spantree [cist | vlan vlan_id] protocol {stp | rstp | mstp}
spantree vlan vlan_id [-vlan_id2] admin-state {enable | disable}
spantree mst region name name
no spantree mst region name
spantree mst region revision-level rev_level
spantree mst region max-hops max_hops
spantree msti msti_id [name name]
no spantree msti msti_id [name]
spantree msti msti_id vlan vlan_id[-vlan_id2]
no spantree msti msti_id vlan vlan_id[-vlan_id2]
spantree [cist | msti msti_id | vlan vlan_id] [port slot/port[-port2] / linkagg linkagg_id[-
linkagg_id2]] priority priority
spantree [cist | vlan vlan_id] hello-time seconds
spantree [cist | vlan vlan_id] max-age seconds
spantree [cist | vlan vlan_id] forward-delay seconds
spantree {vlan vlan_id | cist} bpdu-switching {enable | disable}
spantree path-cost-mode {auto | 32bit}
spantree pvst+compatibility {port slot/port] | linkagg linkagg_id] {enable | disable | auto}

```

```

spantree [msti msti_id] auto-vlan-containment {enable | disable}
spantree cist {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} {enable | disable}
spantree vlan vlan_id [-vlan2] {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]}
{enable | disable}
spantree cist {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} path-cost
path_cost
spantree msti msti_id {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} path-cost
path_cost
spantree vlan vlan_id {port slot/port[-port2] / linkagg linkagg_id [-linkagg_id2]} path-
cost path_cost
spantree cist {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} mode {forwarding
|
dynamic | blocking}
spantree vlan vlan_id {port slot/port[-port2] / linkagg linkagg_id [-linkagg_id2]} mode
{dynamic | blocking | forwarding}
spantree cist {port slot/port [-port2] | linkagg linkagg_id [-linkagg_id2]} connection
{noptp | ptp | autoptp}
spantree vlan vlan_id {port slot/port [-port2] / linkagg linkagg_id [-linkagg_id2]}
connection {noptp | ptp | autoptp}
spantree cist {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} admin-edge
{enable | disable}
spantree vlan vlan_id {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} admin-
edge {enable | disable}
spantree cist {port slot/port[-port2] / linkagg linkagg_id [-linkagg_id2]} auto-edge {enable
| disable}
spantree vlan vlan_id {port slot/port[-port2] / linkagg linkagg_id [-linkagg_id2]} auto-
edge {enable | disable}
spantree cist {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} restricted-role
{enable | disable}
spantree vlan vlan_id {port slot/port[-port2] / linkagg linkagg_id[-linkagg_id2]} restricted-
role {enable | disable}
spantree cist {port slot/port[-port2] | linkagg linkagg_id[-linkagg_id2]} restricted-tcn
{enable | disable}
spantree vlan vlan_id {port slot/port [-port2] / linkagg linkagg_id [-linkagg_id2]}
restricted-tcn {enable | disable}
spantree cist txholdcount value
spantree vlan vlan_id txholdcount {value}
show spantree
show spantree cist
show spantree msti [msti_id]
show spantree vlan [vlan_id]
show spantree ports [forwarding | blocking | active | configured]
show spantree cist ports [forwarding | blocking | active | configured]
show spantree msti [msti_id] ports [forwarding | blocking | active | configured]

```



```

show spantree vlan [vlan_id[-vlan_id2]] ports [forwarding | blocking | active | configured]
show spantree mode
show spantree mst {region | port slot/port / linkagg linkagg_id}
show spantree msti [msti_id] vlan-map
show spantree cist vlan-map
show spantree [vlan vlan_id] map-msti

```

Shortest Path Bridging Commands

```

spb bvlan {bvlan_id[-bvlan_id2]} [admin-state {enable | disable}] [name description]
    [tunnel-mtu mtu]
no spb bvlan bvlan_id
spb isis bvlan bvlan_id ect-id ect_id
spb isis control-bvlan bvlan_id
spb isis bvlan bvlan_id tandem-multicast-mode {sgmode | gmode}
spb isis bridge-priority priority
spb isis interface {port slot/port[-port2] | linkagg agg_id[-agg_id2]} [admin-state {enable |
    disable}] [hello-interval seconds] [hello-multiplier count] [metric metric]
no spb isis interface [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]
spb isis admin-state {enable | disable}
spb isis area-address area_address
spb isis source-id {source_id | auto}
spb isis spf-wait [initial-wait milliseconds | second-wait milliseconds | max-wait milliseconds]
spb isis lsp-wait {max-wait milliseconds | initial-wait milliseconds | second-wait
    milliseconds}
spb isis overload [timeout seconds]
no spb isis overload
spb isis overload-on-boot [timeout seconds]
no spb isis overload-on-boot
spb isis graceful-restart
no spb isis graceful-restart
spb isis graceful-restart helper {enable | disable}
show spb isis info
show spb isis interface

```

Link Aggregation Commands

```

linkagg static agg agg_num1 [-agg_num2] size size [name name] [admin-state {enable |
    disable}] [multi-chassis active] [hash (source-mac | destination-mac | source-and-
    destination-mac | source-ip | destination-ip | source-and-destination-ip)]
no linkagg static agg agg_num1 [-agg_num2]
linkagg static agg agg_num1 [-agg_num2] name name
no linkagg static agg agg_num1 [-agg_num2] name
linkagg static agg agg_num1 [-agg_num2] admin-state {enable | disable}

```

```

linkagg static port slot/port[-port2] agg agg_num
no linkagg static port slot/port[-port2]
linkagg lacp agg agg_num1 [-agg_num2] size size
no linkagg lacp agg agg_num1 [-agg_num2] size size
linkagg lacp agg agg_num name name
no linkagg lacp agg agg_num1 [-agg_num2] name
linkagg lacp agg agg_num1 [-agg_num2] admin-state {enable | disable}
linkagg lacp agg agg_num1 [-agg_num2] actor admin-key actor_admin_key
no linkagg lacp agg agg_num1 [-agg_num2] actor admin-key
linkagg lacp agg agg_num1 [-agg_num2] actor system-priority actor_system_priority
no linkagg lacp agg agg_num1 [-agg_num2] actor system-priority
no linkagg lacp agg agg_num1 [-agg_num2] actor system-id
linkagg lacp agg agg_num1 [-agg_num2] partner system-id partner_system_id
no linkagg lacp agg agg_num1 [-agg_num2] partner system-id
linkagg lacp agg agg_num1 [-agg_num2] partner system-priority partner_system_priority
no linkagg lacp agg agg_num1 [-agg_num2] partner system-priority
linkagg lacp agg agg_num1 [-agg_num2] partner admin-key partner_admin_key
no linkagg lacp agg agg_num1 [-agg_num2] partner admin-key
linkagg lacp port slot/port[-port2] actor admin-key actor_admin_key
no linkagg lacp port slot/port[-port2] [actor admin-state {[active] [timeout] [aggregate]
    [synchronize] [collect] [distribute] [default] [expire] | none}]
linkagg lacp port slot/port[-port2] actor admin-state {[active] [timeout] [aggregate]
    [synchronize] [collect] [distribute] [default] [expire] | none}
no linkagg lacp port slot/port[-port2] actor admin-state {[active] [timeout] [aggregate]
    [synchronize]
    [collect] [distribute] [default] [expire] | none}
linkagg lacp port slot/port[-port2] actor system-id actor_system_id
no linkagg lacp port slot/port[-port2] actor system-id
linkagg lacp port slot/port[-port2] actor system-priority actor_system_priority
no linkagg lacp port slot/port[-port2] actor system-priority
linkagg lacp port slot/port[-port2] partner admin-state
    {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] |
    none}
no linkagg lacp port slot/port[-port2] partner admin-state
    {[ active] [ timeout] [aggregate] [synchronize] [collect] [distribute]
    [default] [expire] | none}
linkagg lacp port slot/port[-port2] partner admin system-id partner_admin_system_id
no linkagg lacp port slot/port[-port2] partner admin system-id
linkagg lacp port slot/port[-port2] partner admin-key partner_admin_key
no linkagg lacp port slot/port[-port2] partner admin-key
linkagg lacp port slot/port[-port2] partner admin system-priority
    partner_admin_system_priority
no linkagg lacp port slot/port[-port2] partner admin system-priority
linkagg lacp port slot/port[-port2] actor port-priority actor_port_priority

```

```

no linkagg lacp port slot/port[-port2] actor port-priority
linkagg lacp port slot/port[-port2] partner admin-port partner_admin_port
no linkagg lacp port slot/port[-port2] partner admin-port
linkagg lacp port slot/port[-port2] partner admin port-priority partner_admin_port_priority
no linkagg lacp port slot/port[-port2] partner admin port-priority
linkagg range local {agg_num-agg_num | none} peer {agg_num-agg_num | none} multi-
  chassis {agg_num-agg_num | none}
show linkagg {agg [agg_num1 [-agg_num2]}
show linkagg {agg agg_num1 [-agg_num2]} port [slot/port]
show linkagg range [operation | config]

```

Multi-Chassis Commands

```

multi-chassis chassis-id chassis_id
no multi-chassis chassis-id
multi-chassis hello-interval seconds
multi-chassis ipc-vlan vlan_id
multi-chassis chassis-group group_id
no multi-chassis chassis-group
multi-chassis loop-detection {enable | disable}
multi-chassis loop-detection transmit-interval seconds
multi-chassis vf-link create
no multi-chassis vf-link
multi-chassis vf-link member-port slot/port
no multi-chassis vf-link member-port slot/port
multi-chassis vf-link default-vlan vlan_id
no multi-chassis vf-link default-vlan
multi-chassis vip-vlan vlan_id[-vlan_id2]
no multi-chassis vip-vlan vlan_id[-vlan_id2]
show multi-chassis status
show multi-chassis loop-detection
show multi-chassis vf-link
show multi-chassis vf-link member-port [slot/port]
show multi-chassis consistency
show multi-chassis consistency linkagg [agg_id [vlan-list] | vlan-list]
clear multi-chassis loop-detection

```

Ethernet Ring Protection Commands

```

erp-ring ring_id port1 {slot/port | linkagg agg_num} port2 {slot/port | linkagg agg_num}
  service-vlan vlan_id level level_num [guard-timer guard_timer] [wait-to-
  restore-timer wtr_timer] [enable | disable]
no erp-ring ring_id
erp-ring ring_id rpl-node {port slot/port | linkagg agg_num}

```

```

no erp-ring ring_id rpl-node
erp-ring ring_id wait-to-restore wtr_timer
no erp-ring ring_id wait-to-restore
erp-ring ring_id {enable | disable}
erp-ring ring_id guard-timer guard_timer
no erp-ring ring_id guard-timer
Creates an Ethernet Ring Protection (ERP) sub-ring.
erp-ring ring_id sub-ring-port {slot/port | linkagg agg_num} service-vlan vlan_id level
  level_num [guard-timer guard_timer] [wait-to-restore-timer wtr_timer]
  [enable | disable]
erp-ring ring_id virtual-channel [enable | disable]
Enables or Disables revertive mode on the specified node.
erp-ring ring_id revertive [enable | disable]
Clears any pending state (for example, non-revertive restoring).
erp-ring ring_id clear
Configures a ring port to accept a “loss of connectivity” event from Ethernet OAM for a
  remote endpoint.
erp-ring ring_id ethoam-event {slot/port | linkagg agg_num} remote-endpoint mep_id
no erp-ring ring_id ethoam-event {slot/port | linkagg agg_num}
Clears ERP statistics for all rings, a specific ring, or a specific ring port.
clear erp statistics [ring ring_id [port slot/port | linkagg agg_num]]
show erp [ring ring_id | [port slot/port | linkagg agg_num]]
show erp statistics [ring ring_id [port slot/port | linkagg agg_num]]

```

MVRP Commands

```

mvrp {enable | disable}
mvrp port slot/port [- port2] {enable | disable}
mvrp linkagg agg_num [-agg_num2] {enable | disable}
mvrp {port slot/port [- port2] | linkagg agg_num [-agg_num2]} registration {normal | fixed |
  forbidden}
mvrp {port slot/port [- port2] | linkagg agg_num [-agg_num2]} applicant {participant |
  non-participant | active}
mvrp {port slot/port [- port2] | linkagg agg_num [-agg_num2]} restrict-vlan-registration vlan
  vlan_list
no mvrp {port slot/port [- port2] | linkagg agg_num [-agg_num2]} restrict-vlan-registration
  vlan
  vlan_list
mvrp {port slot/port [- port2] | linkagg agg_num [-agg_num2]} restrict-vlan-advertisement
  vlan vlan_list
no mvrp {port slot/port [- port2] | linkagg agg_num [-agg_num2]} restrict-vlan-advertisement
  vlan vlan_list
mvrp {linkagg agg_num [-agg_num2] | port slot/port [- port2]} static-vlan-restrict vlan
  vlan_list

```

```

no mvrp {linkagg agg_num [-agg_num2] | port slot/port [-port2]} static-vlan-restrict vlan
    vlan_list
show mvrp configuration
show mvrp port {slot/port [-port2]} [enable | disable]
show mvrp linkagg [agg_num [-agg_num2]] [enabled | disabled]
mvrp [port slot/port [-port2] | linkagg agg_num [-agg_num2]] clear-statistics

```

802.1AB Commands

```

lldp transmit interval seconds
lldp transmit hold-multiplier num
lldp transmit delay seconds
lldp reinit delay seconds
lldp notification interval seconds
lldp {port slot/port [-port] | slot slot | chassis} lldpdu {tx | rx | tx-and-rx | disable}
lldp {port slot/port [-port] | slot slot | chassis} notification {enable | disable}
lldp {port slot/port [-port] | slot slot | chassis} tlv management {port-description | system-
    name | system-description | system-capabilities | management-address} {enable |
    disable}
lldp {port slot/port [-port] | slot slot | chassis} tlv dot1 {port-vlan | vlan-name} {enable |
    disable}
lldp {port slot/port [-port] | slot slot | chassis} tlv dot3 mac-phy {enable | disable}
lldp {port slot/port [-port] | slot slot | chassis} tlv med {power | capability} {enable | disable}
show lldp system-statistics
show lldp [port slot/port [-port]] statistics
show lldp local-system
show lldp [port slot/port [-port]] | slot slot] local-port
show lldp local-management-address
show lldp [port slot/port [-port] | slot slot] remote-system
show lldp { slot | slot/port [-port]} config
show lldp [port slot/port [-port] slot slot] statistics
show lldp [slot/port [-port] | slot] remote-system [med {network-policy | inventory}]

```

IP Commands

```

ip interface {name / emp} [{address | vip-address] ip_address [mask subnet_mask] [admin-
    state [enable | disable]] [vlan vlan_id] [forward | no forward] [local-proxy-arp | no local-
    proxy-arp] [e2 | snap] [primary | no primary]
no ip interface name
ip interface name tunnel [source ip_address] [destination ip_address] [protocol {ipip | gre}]
ip router primary-address ip_address
ip router router-id ip_address
ip static-route ip_address [mask mask] gateway gateway/follows ip_address [metric metric]

```

```

no ip static-route ip_address [mask mask] gateway ip_address/follows ip_address [metric
    metric]
[vrf name] ip route-pref {static | rip | ospf | isisL2 | isisL1 | ibgp | ebgp | import} value
ip default-ttl hops
ping {ip_address | hostname} [source-interface ip_interface] [count count] [size packet_size]
    [interval seconds] [timeout seconds] [data-pattern string] [dont-fragment] [tos tos_val]
traceroute {ip_address | hostname} [max-hop max_hop_count] [min-hop min_hop_count]
    [source-interface ip_interface] [probes probe_count] [timeout seconds] [port
    port_number_value]
ip directed-broadcast {on | off}
[vrf name] ip service {all | service_name / port service_port} admin-state {enable | disable}
ip service {service_name} port {default | service_port}
[vrf name] ip redistribute {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp}
    route-map route-map-name [status {enable | disable}]
no ip redistribute {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} [route-map
    route-map-name]
ip access-list access-list-name
no ip access-list access-list-name
ip access-list access-list-name address address/prefixLen [action {permit | deny}]
    [redist-control {all-subnets | no-subnets | aggregate}]
no ip access-list access-list-name address address/prefixLen
ip route-map route-map-name [sequence-number number] match ip-nexthop
    {access-list-name | ip_address/prefixLen [permit | deny]}
no ip route-map route-map-name [sequence-number number] match ip-nexthop
    {access-list-name | ip_address/prefixLen [permit | deny]}
ip route-map route-map-name [sequence-number number] match ipv6-nexthop
    {access-list-name | ipv6_address/prefixLen [permit | deny]}
no ip route-map route-map-name [sequence-number number] match ipv6-nexthop
    {access-list-name | ipv6_address/prefixLen [permit | deny]}
ip route-map route-map-name [sequence-number number] match ipv4-interface interface-
    name
no ip route-map route-map-name [sequence-number number] match ipv4-interface interface-
    name
ip route-map route-map-name [sequence-number number] match ipv6-interface interface-
    name
no ip route-map route-map-name [sequence-number number] match ipv6-interface interface-
    name
ip route-map route-map-name [sequence-number number] match metric metric [deviation
    deviation]
no ip route-map route-map-name [sequence-number number] match metric metric
    [deviation deviation]
ip route-map route-map-name [sequence-number number] match route-type {internal |
    external [type1 | type2] | level1 | level2}

```

```

no ip route-map route-map-name [sequence-number number] match route-type {internal |
external [type1 | type2] | level1 | level2}
ip route-map route-map-name [sequence-number number] match protocol {local | static | rip
| ospf | isis | bgp}
no ip route-map route-map-name [sequence-number number] match protocol {local | static |
rip | ospf | isis | bgp}
ip route-map route-map-name [sequence-number number] set metric metric
[effect {add | subtract | replace | none}]
no ip route-map route-map-name [sequence-number number] set metric metric
[effect {add | subtract | replace | none}]
ip route-map route-map-name [sequence-number number] set metric-type
{internal | external [type1 | type2]}
no ip route-map route-map-name [sequence-number number] set metric-type
{internal | external [type1 | type2]}
ip route-map route-map-name [sequence-number number] set tag tag-number
no ip route-map route-map-name [sequence-number number] set tag tag-number
ip route-map route-map-name [sequence-number number] set community community-string
no ip route-map route-map-name [sequence-number number] set community community-
string
ip route-map route-map-name [sequence-number number] set local-preference value
no ip route-map route-map-name [sequence-number number] set local-preference value
ip route-map route-map-name [sequence-number number] set level {level1 | level2 | level1-2}
no ip route-map route-map-name [sequence-number number] set level {level1 | level2 |
level1-2}
ip route-map route-map-name [sequence-number number] set ip-nexthop ip_address
no ip route-map route-map-name [sequence-number number] set ip-nexthop ip_address
ip route-map route-map-name [sequence-number number] set ipv6-nexthop ipv6_address
no ip route-map route-map-name [sequence-number number] set ipv6-nexthop ipv6_address
vrf [name / default]
no vrf name
[vrf name] ip export route-map route-map-name
[vrf name] no ip export
[vrf name] ip import vrf {name | default} route-map route-map-name
[vrf name] no ip import vrf {name | default}
[vrf name] show ip export
[vrf name] show ip import
show ip global-route-table [export-vrf name]
arp ip_address hardware_address [alias] [arp-name name] [port slot/port] [linkagg agg_num]
no arp ip_address [alias]
clear arp-cache
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
arp filter ip_address [mask ip_mask] [vlan_id] [sender | target] [allow | block]

```

```

no arp filter ip_address
clear arp-cache
icmp type type code code {{enable | disable} | min-pkt-gap gap}
icmp unreachable [net-unreachable | host-unreachable | protocol-unreachable |
port-unreachable] {{enable | disable} | min-pkt-gap gap}
icmp echo [request | reply] {{enable | disable} | min-pkt-gap gap}
icmp timestamp [request | reply] {{enable | disable} | min-pkt-gap gap}
icmp add-mask [request | reply] {{enable | disable} | min-pkt-gap gap}
icmp messages {enable | disable}
ip dos scan close-port-penalty penalty_value
ip dos scan tcp open-port-penalty penalty_value
ip dos scan udp open-port-penalty penalty_value
ip dos scan threshold threshold_value
ip dos trap {enable | disable}
ip dos scan decay decay_value
show ip traffic
show ip interface [name / emp | vlan vlan id]
[vrf name] show ip routes [summary]
[vrf name] show ip route-pref
[vrf name] show ipv6 redist [rip | ospf | isis | bgp]
show ip access-list [access-list-name]
show ip route-map [route-map-name]
[vrf name] show ip router database [protocol type / gateway ip_address / dest {ip_address/
prefixLen / ip_address}]
show ip emp-routes
show ip config
show ip protocols
show ip router-id
show ip service
show ip dos arp-poison
show arp [ip_address | hardware_address]
show arp filter [ip_address]
show icmp control
show icmp [statistics]
show tcp statistics
show tcp ports
show udp statistics
show udp ports
show ip dos config
show ip dos statistics
show vrf

```

IPv6 Commands

```
ipv6 interface if_name [vlan vid | tunnel {tid | 6to4}] admin-state [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-min-interval interval | no ra-min-interval]
[ra-clock-skew time]
[ra-send-mtu] {yes | no}
[mtu size]
[retrans-timer time]
[dad-transmits count]
[ra-hop-limit count]
no ipv6 interface if_name
ipv6 interface if_name tunnel {[source ipv4_source] [destination ipv4_destination]}
ipv6 address ipv6_address /prefix_length [anycast] {if_name | loopback}
no ipv6 address ipv6_address [anycast] {if_name | loopback}
ipv6 address ipv6_prefix eui-64 {if_name | loopback}
no ipv6 address ipv6_prefix eui-64 {if_name | loopback}
ipv6 address global-id {generate | globalID}
ipv6 address local-unicast [global-id globalID] [subnet-id subnetID] {interface-id interfaceID
    | eui-64} [prefix-length prefixLength] {if-name | loopback}
[no] ipv6 address local-unicast [global-id globalID] [subnet-id subnetID] {interface-id
    interfaceID | eui-64} [prefix-length prefixLength] {if-name | loopback}
ipv6 dad-check ipv6_address if_name
ipv6 hop-limit value
no ipv6 hop-limit
ipv6 pmtu-lifetime time
ipv6 neighbor stale-lifetime stale-lifetime
ipv6 neighbor ipv6_address hardware_address {if_name} {port slot/port/linkagg num}
no ipv6 neighbor ipv6_address {if_name}
ipv6 prefix ipv6_address /prefix_length if_name
    [valid-lifetime time]
    [preferred-lifetime time]
    [on-link-flag {true | false}]
    [autonomous-flag {true | false}] if_name
no ipv6 prefix ipv6_address /prefix_length if_name
ipv6 static-route ipv6_prefix/prefix_length gateway ipv6_address [if_name] [metric metric]
no ipv6 static-route ipv6_prefix/prefix_length gateway ipv6_address [if_name]
```

```
ipv6 route-pref {static | ospf | rip | ebgp | ibgp} value
ipv6 virtual-source-mac {on | off}
ping6 {ipv6_address | hostname} [if_name] [count count] [size data_size] [interval seconds]
traceroute6 {ipv6_address | hostname} [if_name] [max-hop hop_count] [dest-port
    port_number] [probe-count probe] [size size] [host-names {yes|no}]
show ipv6 icmp statistics [if_name]
show ipv6 interface [if_name | loopback]
show ipv6 pmtu table
show ipv6 neighbors [ipv6_prefix/prefix_length | if_name | hw hardware_address | static]
clear ipv6 neighbors
show ipv6 prefixes
show ipv6 routes [ipv6_prefix/prefix_length | static]
show ipv6 route-pref
show ipv6 router database [protocol type / gateway ipv6_address / dest ipv6_prefix/
    prefix_length]
show ipv6 tcp connections
show ipv6 tcp listeners
show ipv6 traffic [if_name]
show ipv6 tunnel configured
show ipv6 tunnel 6to4
show ipv6 udp ports
show ipv6 information
ipv6 redistrib {local | static | rip | ospf | isis | bgp} into {rip | ospf | isis | bgp} route-map route-
    map-name
    [admin-state {enable | disable}]
ipv6 access-list access-list-name
no ipv6 access-list access-list-name
ipv6 access-list access-list-name address address/prefixLen [action {permit | deny}]
    [redist-control {all-subnets | no-subnets | aggregate}]
no ipv6 access-list access-list-name address address/prefixLen
show ipv6 redistrib [rip | ospf | bgp]
show ip access-list [access-list-name]
ipv6 load rip
ipv6 rip admin-state {enable | disable}
ipv6 rip invalid-timer seconds
ipv6 rip garbage-timer seconds
ipv6 rip holddown-timer seconds
ipv6 rip jitter value
ipv6 rip route-tag value
ipv6 rip update-interval seconds
ipv6 rip triggered-sends {all | updated-only | none}
ipv6 rip interface if_name
[no] ipv6 rip interface if_name
ipv6 rip interface if_name metric value
```

```

ipv6 rip interface if_name rcv-status {enable | disable}
ipv6 rip interface if_name send-status {enable | disable}
ipv6 rip interface if_name horizon {none | split-only | poison}
show ipv6 rip
show ipv6 rip interface [if_name]
show ipv6 rip peer [ipv6_addresses]
show ipv6 rip routes [dest <ipv6_prefix/prefix_length>] | [gateway <ipv6_addr>] | [detail
<ipv6_prefix/prefix_length>]

```

IPsec commands

```

ipsec key name {sa-authentication | sa-encryption} [encrypted] key
no ipsec key name {sa-authentication | sa-encryption}
ipsec security-key [old_key] new_key
ipsec policy name [priority priority] [source {ipv6_address [/prefix_length]} [port
port]] [destination {ipv6_address [/prefix_length]} [port port]] [protocol {any
| icmp6 [type type] | tcp | udp | ospf | vrrp | number protocol}] [in | out]
[discard | ipsec | none] [description description] [admin-state {enable |
disable}]
no ipsec policy name
ipsec policy name rule index [ah | esp]
no ipsec policy name
ipsec sa name {esp | ah} [source ipv6_address ] [destination ipv6_address] [spi spi]
[encryption {null | 3des-cbc | aes-cbc [key-size key_length]}]
[authentication {none | hmac-md5 | hmac-sha1 | aes-xcbc-mac}]
[description description] [admin-state {enable | disable}]
no ipsec sa name
show ipsec policy [name]
show ipsec sa [name | esp | ah]
show ipsec key [sa-encryption | sa-authentication]
show ipsec ipv6 statistics

```

RIP Commands

```

ip load rip
ip rip admin-state {enable | disable}
ip rip interface {interface_name}
no ip rip interface {interface_name}
ip rip interface {interface_name} admin-state {enable | disable}
ip rip interface {interface_name} metric value
ip rip interface {interface_name} send-version {none | v1 | v1compatible | v2}
ip rip interface {interface_name} rcv-version {v1 | v2 | both | none}
ip rip interface {interface_name} ingress-filter {filter_name}
ip rip interface {interface_name} ingress-filter {filter_name}

```

```

ip rip interface {interface_name} egress-filter {filter_name}
ip rip force-holddowntimer seconds
ip rip host-route
no ip rip host-route
ip rip route-tag value
ip rip interface {interface_name} auth-type {none | simple | md5}
ip rip interface {interface_name} auth-key string
ip rip update-interval seconds
ip rip invalid-timer seconds
ip rip garbage-timer seconds
ip rip holddown-timer seconds
show ip rip
show ip rip routes [ip_address ip_mask]
show ip rip interface [interface_name]
show ip rip peer [ip_address]

```

BFD Commands

```

ip bfd admin-state {enable | disable}
ip bfd transmit transmit_interval
ip bfd receive receive_interval
ip bfd multiplier num
ip bfd echo-interval echo_interval
ip bfd interface if_name
no ip bfd interface if_name
ip bfd interface if_name admin-state {enable | disable}
ip bfd interface if_name transmit transmit_interval
ip bfd interface if_name receive receive_interval
ip bfd interface if_name multiplier num
ip bfd interface if_name echo-interval echo_interval
ip ospf bfd-state {enable | disable}
ip ospf bfd-state all-interfaces {enable | disable}
ip ospf interface if_name bfd-state {enable | disable}
ip ospf interface if_name bfd-state drs-only
ip ospf interface if_name bfd-state all-neighbors {enable | disable}
ip bgp bfd-state {enable | disable}
ip bgp bfd-state all-neighbors {enable | disable}
ip bgp neighbor ipv4_address bfd-state {enable | disable}
vrrp bfd-state {enable | disable}
vrrp track track_id address ipv4_address bfd-state {enable| disable}
show ip bfd
show ip bfd interfaces [if_name]
show ip bfd sessions [session_num] [slot slot_num]
show ip bfd sessions statistics session_num

```

```
ip static-route all bfd-state {enable| disable}
ip static-route ipv4_prefix/px_length gateway ipv4_host_address bfd-state {enable| disable}
```

DHCP Relay Commands

```
ip helper address ip_address
no ip helper address [ip_address]
ip helper vlan vlan_id[-vlan_id2] address ip_address
no ip helper vlan vlan_id[-vlan_id2] address ip_address
ip helper standard
ip helper per-vlan-only
ip helper forward-delay seconds
ip helper maximum-hops hops
ip helper agent-information {enable | disable}
ip helper agent-information policy {drop | keep | replace}
ip helper pxe-support {enable | disable}
ip helper boot-up {enable | disable}
ip helper boot-up enable {BOOTP | DHCP}
ip udp relay port port_num [description description]
ip udp relay no port port_num
ip udp relay service {TFTP | TACACS | NTP | NBNS | NBDD | DNS} [description
description]
ip udp relay no service {TFTP | TACACS | NTP | NBNS | NBDD | DNS}
ip udp relay service {TFTP | TACACS | NTP | NBNS | NBDD | DNS} | port port_num
[description description] vlan vlan_id[-vlan_id2]
ip udp relay service {TFTP | TACACS | NTP | NBNS | NBDD | DNS} | port port_num no vlan
vlan_id[-vlan_id2]
show ip helper
show ip helper statistics
show ip udp relay [service {TFTP | TACACS | NTP | NBNS | NBDD | DNS} | port port_num]
show ip udp relay statistics [service {TFTP | TACACS | NTP | NBNS | NBDD | DNS}] [port
[port_num]]
ip udp relay no statistics
```

VRRP Commands

```
vrrp vrid vlan_id admin-state [enable | disable] [priority priority] [preempt | no preempt]
[[advertising] interval seconds]
no vrrp vrid vlan_id
vrrp vrid vlan_id address ipv4Addr
vrrp vrid vlan_id no address ipv4Addr
vrrp track track_id admin-state [enable | disable] [priority value] [ipv4-interface name | ipv6-
interface name | port slot/port | address address]
no vrrp track track_id
```

```
vrrp vrid vlan_id track-association track_id
vrrp vrid vlan_id no track-association track_id
vrrp trap
no vrrp trap
vrrp delay seconds
vrrp3 vrid vlan_id admin-state [enable | disable] [priority priority] [preempt | no
preempt][accept | no accept] [[advertising] interval centiseconds]
no vrrp3 vrid vlan_id
vrrp3 vrid vlan_id address [ipv6Addr | ipv6v4Addr]
vrrp3 vrid vlan_id no address [ipv6Addr | ipv6v4Addr]
vrrp3 trap
no vrrp3 trap
vrrp3 vrid vlan_id track-association track_id
vrrp3 vrid vlan_id no track-association track_id
show vrrp [vrid]
show vrrp [vrid] statistics
show vrrp track [track_id]
show vrrp [vrid] track-association [track_id]
show vrrp3 [vrid]
show vrrp3 [vrid] statistics
show vrrp3 [vrid] track-association [track_id]
```

OSPF Commands

```
ip ospf admin-state {enable | disable}
ip load ospf
ip ospf asbr
no ip ospf asbr
ip ospf exit-overflow-interval seconds
ip ospf extlsdb-limit limit
ip ospf host ip_address tos tos [metric metric]
no ip ospf host ip_address tos tos
ip ospf mtu-checking
no ip ospf mtu-checking
ip ospf default-originate {only | always} [metric-type {type1 | type2}] [metric value]
no ip ospf default-originate
ip ospf route-tag tag
ip ospf spf-timer [delay delay_seconds] [hold hold_seconds]
ip ospf virtual-link area_id router_id [auth-type {none | simple | md5}] [auth-key key_string]
[dead-interval seconds] [hello-interval seconds] [retrans-interval seconds] [transit-delay
seconds]
no ip ospf virtual-link area_id router_id
ip ospf neighbor neighbor_id {eligible | non-eligible}
no ip ospf neighbor neighbor_id
```

```

ip ospf area area_id [summary {enable | disable}] | [type {normal | stub | nssa}]
no ip ospf area area_id
ip ospf area area_id default-metric tos [[cost cost] | [type {ospf | type 1 | type 2}]]
no ip ospf area area_id default-metric tos
ip ospf area area_id range {summary | nssa} ip_address subnet_mask
    [effect {admatching | noMatching}]
no ip ospf area area_id range {summary | nssa} ip_address subnet_mask
ip ospf interface {interface_name}
no ip ospf interface {interface_name}
ip ospf interface {interface_name} admin-state {enable | disable}
no ip ospf interface {interface_name} admin-state {enable | disable}
ip ospf interface {interface_name} area area_id
ip ospf interface {interface_name} auth-key key_string
ip ospf interface {interface_name} auth-type [none | simple | md5]
ip ospf interface {interface_name} dead-interval seconds
ip ospf interface {interface_name} hello-interval seconds
ip ospf interface {interface_name} md5 key_id [enable | disable]
ip ospf interface {interface_name} md5 key_id key key_string
ip ospf interface {interface_name} type {point-to-point | point-to-multipoint | broadcast | non-
    broadcast}
ip ospf interface {interface_name} cost cost
ip ospf interface {interface_name} poll-interval seconds
ip ospf interface {interface_name} priority priority
ip ospf interface {interface_name} retrans-interval seconds
ip ospf interface {interface_name} transit-delay seconds
ip ospf restart-support {planned-unplanned | planned-only}
no ip ospf restart-support
ip ospf restart-interval [seconds]
ip ospf restart-helper [admin-state {enable | disable}]
ip ospf restart-helper strict-lsa-checking admin-state {enable | disable}
ip ospf restart initiate
show ip ospf
show ip ospf border-routers [area_id] [router_id] [tos] [gateway]
show ip ospf ext-lsdb [linkstate-id ls_id] [router-id router_id]
show ip ospf host [ip_address]
show ip ospf lsdb [area_id] [rtr | net | netsum | asbrsum] [linkstate-id ls_id] [router-id
    router_id]
show ip ospf neighbor [ip_address]
show ip ospf routes [ip_addr mask tos gateway]
show ip ospf virtual-link [router_id]
show ip ospf virtual-neighbor area_id router_id
show ip ospf area [area_id]
show ip ospf area area_id range [{summary | nssa} ip_address ip_mask]
show ip ospf area area_id stub

```

```

show ip ospf interface [interface_name]
show ip ospf restart

```

OSPFv3 Commands

```

ipv6 ospf admin-state {enable | disable}
ipv6 load ospf
ipv6 ospf host ipv6_address [area area_id] [metric metric]
no ipv6 ospf host ipv6_address area area_id
ipv6 ospf mtu-checking
no ipv6 ospf mtu-checking
ipv6 ospf route-tag tag
ipv6 ospf spf-timer [delay delay_seconds] [hold hold_seconds]
ipv6 ospf virtual-link area area_id router router_id
    [dead-interval seconds] [hello-interval seconds] [retrans-interval seconds] [transit-delay
    seconds]
no ipv6 ospf virtual-link area area_id router router_id
ipv6 ospf area area_id [type {normal | stub [default-metric metric]}]
no ipv6 ospf area area_id
ipv6 ospf interface interface_name
no ipv6 ospf interface interface_name
ipv6 ospf interface interface_name admin-state {enable | disable}
no ipv6 ospf interface interface_name
ipv6 ospf interface interface_name area area_id
ipv6 ospf interface interface_name dead-interval seconds
ipv6 ospf interface interface_name hello-interval seconds
ipv6 ospf interface interface_name cost cost
ip ospf interface interface_name priority priority
ipv6 ospf interface interface_name retrans-interval interval
ipv6 ospf interface interface_name transit-delay delay
show ipv6 ospf
show ipv6 ospf border-routers [area area_id] [router router_id]
show ipv6 ospf host [ipv6_address]
show ipv6 ospf lsdb [area area_id] [rtr | net | netsum | asbrsum] [linkstate-id ls_id] [router-id
    router_id]
show ipv6 ospf neighbor [router ipv4_address][interface interface_name]
show ipv6 ospf routes [prefix ipv6_address_prefix][gateway gateway]
show ipv6 ospf virtual-link [router_id]
show ipv6 ospf area [area_id]
show ipv6 ospf interface [interface_name]

```


BGP Commands

```
ip load bgp
ip bgp admin-state {enable | disable}
ip bgp autonomous-system value
ip bgp bestpath as-path ignore
no ip bgp bestpath as-path ignore
ip bgp cluster-id ip_address
ip bgp default local-preference value
ip bgp fast-external-failover
no ip bgp fast-external-failover
ip bgp always-compare-med
no ip bgp always-compare-med
ip bgp bestpath med missing-as-worst
no ip bgp bestpath med missing-as-worst
ip bgp client-to-client reflection
no ip bgp client-to-client reflection
ip bgp as-origin-interval seconds
no ip bgp as-origin-interval
ip bgp synchronization
no ip bgp synchronization
ip bgp confederation identifier value
ip bgp maximum-paths
no ip bgp maximum-paths
ip bgp log-neighbor-changes
no ip bgp log-neighbor-changes
ip bgp dampening [half-life half_life reuse reuse suppress suppress max-suppress-time
    max_suppress_time]
no ip bgp dampening
ip bgp dampening clear
ip bgp aggregate-address ip_address ip_mask
no ip bgp aggregate-address ip_address ip_mask
ip bgp aggregate-address ip_address ip_mask admin-state {enable | disable}
ip bgp aggregate-address ip_address ip_mask as-set
no ip bgp aggregate-address ip_address ip_mask as-set
ip bgp aggregate-address ip_address ip_mask community string
ip bgp aggregate-address ip_address ip_mask local-preference value
no ip bgp aggregate-address ip_address ip_mask local-preference value
ip bgp aggregate-address ip_address ip_mask metric value
no ip bgp aggregate-address ip_address ip_mask metric value
ip bgp aggregate-address ip_address ip_mask summary-only
no ip bgp aggregate-address ip_address ip_mask summary-only
ip bgp network network_address ip_mask
no ip bgp network network_address ip_mask
```

```
ip bgp network network_address ip_mask admin-state {enable | disable}
ip bgp network network_address ip_mask community string
ip bgp network network_address ip_mask local-preference value
no ip bgp network network_address ip_mask local-preference value
ip bgp network network_address ip_mask metric value
no ip bgp network network_address ip_mask metric value
ip bgp neighbor ip_address
no ip bgp neighbor ip_address
ip bgp neighbor ip_address admin-state {enable | disable}
ip bgp neighbor ip_address advertisement-interval value
ip bgp neighbor ip_address clear
ip bgp neighbor ip_address route-reflector-client
no ip bgp neighbor ip_address route-reflector-client
ip bgp neighbor ip_address default-originate
no ip bgp neighbor ip_address default-originate
ip bgp neighbor ip_address timers keepalive holdtime
ip bgp neighbor ip_address conn-retry-interval seconds
ip bgp neighbor ip_address auto-restart
ip bgp neighbor ip_address maximum-prefix maximum [warning-only]
ip bgp neighbor ip_address md5 key {string | none}
ip bgp neighbor ip_address md5 key-encrypt encrypted_string
ip bgp neighbor ip_address ebgp-multihop [ttl]
no ip bgp neighbor ip_address ebgp-multihop
ip bgp neighbor ip_address description string
ip bgp neighbor ip_address next-hop-self
no ip bgp neighbor ip_address next-hop-self
ip bgp neighbor ip_address passive
no ip bgp neighbor ip_address passive
ip bgp neighbor ip_address remote-as value
ip bgp neighbor ip_address remove-private-as
no ip bgp neighbor ip_address remove-private-as
ip bgp neighbor ip_address soft-reconfiguration
no ip bgp neighbor ip_address soft-reconfiguration
ip bgp neighbor ip_address stats-clear
ip bgp confederation neighbor ip_address
no ip bgp confederation neighbor ip_address
ip bgp neighbor ip_address update-source [interface_name]
ip bgp neighbor ip_address in-aspathlist {string / none}
ip bgp neighbor ip_address in-communitylist {string / none}
ip bgp neighbor ip_address in-prefixlist {string / none}
ip bgp neighbor ip_address out-aspathlist {string / none}
ip bgp neighbor ip_address out-communitylist {string / none}
ip bgp neighbor ip_address out-prefixlist {string / none}
ip bgp neighbor ip_address route-map {string | none} {in | out}
```

```

no ip bgp neighbor ip_address route-map {in | out}
ip bgp neighbor ip_address clear soft {in | out}
ip bgp policy aspath-list name "regular_expression"
no ip bgp policy aspath-list name "regular_expression"
ip bgp policy aspath-list name "regular_expression" action {permit | deny}
ip bgp policy aspath-list name "regular_expression" priority value
ip bgp policy community-list name {none | no-export | no-advertise | no-export-subconfed |
  num:num}
no ip bgp policy community-list name {none | no-export | no-advertise | no-export-subconfed
  | num:num}
ip bgp policy community-list name {none | no-export | no-advertise | no-export-subconfed |
  num:num}
  action {permit | deny}
ip bgp policy community-list name {none | no-export | no-advertise | no-export-subconfed |
  num:num}
  match-type {exact | occur}
ip bgp policy community-list name {none | no-export | no-advertise | no-export-subconfed |
  num:num}
  priority value
ip bgp policy prefix-list name ip_address ip_mask
no ip bgp policy prefix-list name ip_address ip_mask
ip bgp policy prefix-list name ip_address ip_mask action {permit | deny}
ip bgp policy prefix-list name ip_address ip_mask ge value
ip bgp policy prefix-list name ip_address ip_mask le value
ip bgp policy prefix6-list pxf_list_name prefix6/pfx_length [action{permit/deny}] [admin-
  state{enable/disable}] [ge[{masklength}]] [le[{masklength}]]
no ip bgp policy prefix6-list pxf_list_name prefix6/pfx_length [action{permit/deny}] [admin-
  state{enable/disable}] [ge[{masklength}]] [le[{masklength}]]
ip bgp policy route-map name sequence_number
ip bgp policy route-map name sequence_number action {permit | deny}
ip bgp policy route-map name sequence_number aspath-list as_name
ip bgp policy route-map name sequence_number asprepend path
ip bgp policy route-map name sequence_number community [none | no-export | no-advertise |
  no-export-subconfed | num:num]
ip bgp policy route-map name sequence_number community-list name
ip bgp policy route-map name sequence_number community-mode {add | replace}
ip bgp policy route-map name sequence_number lpref value
ip bgp policy route-map name sequence_number lpref-mode {none | inc | dec | rep}
ip bgp policy route-map name sequence_number match-community [none | no-export | no-
  advertise | no-export-subconfed | num:num]
ip bgp policy route-map name sequence_number match-mask ip_address
ip bgp policy route-map name sequence_number match-prefix ip_address
ip bgp policy route-map name sequence_number match-regexp "regular_expression"
ip bgp policy route-map name sequence_number med value

```

```

ip bgp policy route-map name sequence_number med-mode {none | inc | dec | rep}
ip bgp policy route-map name sequence_number origin {igr | egr | incomplete | none}
ip bgp policy route-map name sequence_number prefix-list prefix_name
ip bgp policy route-map name sequence_number weight value
ip bgp policy route-map name sequence_number community-strip community_list
show ip bgp
show ip bgp statistics
show ip bgp dampening
show ip bgp dampening-stats [ip_address ip_mask] [peer_address]
show ip bgp path
show ip bgp routes [network_address ip_mask]
show ip bgp aggregate-address [ip_address ip_mask]
show ip bgp network [network_address ip_mask]
show ip bgp neighbors [ip_address]
show ip bgp neighbors policy [ip_address]
show ip bgp neighbors timer [ip_address]
show ip bgp neighbors statistics [ip_address]
show ip bgp policy aspath-list [name] ["regular_expression"]
show ip bgp policy community-list [name] [string]
show ip bgp policy prefix-list [name] [ip_address ip_mask]
show ip bgp policy route-map [name] [sequence_number]
ip bgp graceful-restart
no ip bgp graceful-restart
ip bgp graceful-restart restart-interval [seconds]
ip bgp unicast
no ip bgp unicast
ipv6 bgp unicast
no ipv6 bgp unicast
ip bgp neighbor ip_address activate-ipv6
no ip bgp neighbor ip_address activate-ipv6
ip bgp neighbor ip_address ipv6-nexthop ipv6_address
show ipv6 bgp path [ipv6-addr ipv6_address/prefix_length]
show ipv6 bgp routes
  ipv6 bgp network ipv6_address/prefix_length
no ipv6 bgp network ipv6_address/prefix_length
ipv6 bgp network ipv6_address/prefix_length [community {none | num | num:num}]
ipv6 bgp network ipv6_address/prefix_length [local-preference num]
ipv6 bgp network ipv6_address/prefix_length [metric num]
ipv6 bgp network ipv6_address/prefix_length [admin-state {enable | disable}]
show ipv6 bgp network [ipv6_address/prefix_length]
ipv6 bgp neighbor ipv6_address
no ipv6 bgp neighbor ipv6_address
ipv6 bgp neighbor ipv6_address [activate-ipv6]
no ipv6 bgp neighbor ipv6_address [activate-ipv6]

```

```

ip v6 bgp neighbor ipv6_address [ipv6-nexthop ipv6_address]
ip v6 bgp neighbor ipv6_address [admin-state {enable | disable}]
ip v6 bgp neighbor ipv6_address [remote-as num]
ip v6 bgp neighbor ipv6_address [timers num num]
ip v6 bgp neighbor ipv6_address [maximum-prefix num [warning-only]]
no ip v6 bgp neighbor ipv6_address [maximum-prefix num [warning-only]]
ip v6 bgp neighbor ipv6_address [next-hop-self]
no ip v6 bgp neighbor ipv6_address [next-hop-self]
ip v6 bgp neighbor ipv6_address [conn-retry-interval num]
ip v6 bgp neighbor ipv6_address [default-originate]
no ip v6 bgp neighbor ipv6_address [default-originate]
ip v6 bgp neighbor ipv6_address [update-source interface_name]
no ip v6 bgp neighbor ipv6_address [update-source interface_name]
ip v6 bgp neighbor ipv6_address [ipv4-nexthop ip_address]
show ip v6 bgp neighbors [ipv6_address]
show ip v6 bgp neighbors statistics [ipv6_address]
show ip v6 bgp neighbors policy ipv6_address
show ip v6 bgp neighbors timers [ipv6_address]

```

Server Load Balancing Commands

```

ip slb admin-state {enable | disable}
ip slb reset statistics
ip slb cluster name {vip ip_address | condition string} [13 | 12]
no ip slb cluster name
ip slb cluster cluster_name admin-state {enable | disable}
ip slb cluster cluster_name ping period seconds
ip slb cluster cluster_name ping timeout milliseconds
ip slb cluster cluster_name ping retries count
ip slb cluster cluster_name probe probe_name
ip slb server ip ip_address cluster cluster_name [admin-state {enable | disable}] [weight weight]
no ip slb server ip ip_address cluster cluster_name
ip slb server ip ip_address cluster cluster_name probe probe_name
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
no ip slb probe probe_name
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
timeout seconds
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
period seconds

```

```

ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
port port_number
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
retries retries
ip slb probe probe_name {http | https} username user_name
ip slb probe probe_name {http | https} password password
ip slb probe probe_name {http | https} url url
ip slb probe probe_name {http | https} status status_value
ip slb probe probe_name {tcp | udp} send send_string
ip slb probe probe_name {http | https | tcp | udp} expect expect_string
show ip slb
show ip slb clusters [statistics]
show ip slb cluster name [statistics]
show ip slb cluster name server ip_address
show ip slb servers
show ip slb probes [probe_name]

```

IP Multicast Switching Commands

```

ip multicast [vlan vid] admin-state [{enable | disable}]
ip multicast [vlan vid] querier-forwarding [{enable | disable}]
no ip multicast [vlan vid] querier-forwarding
ip multicast [vlan vid] version [version]
ip multicast max-group [num] [action {none | drop | replace}]
ip multicast vlan vid max-group [num] [action {none | drop | replace}]
ip multicast port slot | port max-group [num] [action {none | drop | replace}]
ip multicast static-neighbor vlan vid {port slot/port / linkagg linkagg}
no ip multicast static-neighbor vlan vid {port slot/port / linkagg linkagg}
ip multicast static-querier vlan vid {port slot/port / linkagg linkagg}
no ip multicast static-querier vlan vid {port slot/port / linkagg linkagg}
ip multicast static-group ip_address vlan vid {port slot/port / linkagg linkagg}
no ip multicast static-group ip_address vlan vid {port slot/port / linkagg linkagg}
ip multicast [vlan vid] query-interval [seconds]
ip multicast [vlan vid] last-member-query-interval [tenths-of-seconds]
ip multicast [vlan vid] query-response-interval [tenths-of-seconds]
ip multicast [vlan vid] unsolicited-report-interval [seconds]
ip multicast [vlan vid] router-timeout [seconds]
ip multicast [vlan vid] source-timeout [seconds]
ip multicast [vlan vid] querying [{enable | disable}]
no ip multicast [vlan vid] querying
ip multicast [vlan vid] robustness [robustness]
ip multicast [vlan vid] spoofing [{enable | disable}]

```

```

no ip multicast [vlan vid] spoofing
ip multicast [vlan vid] zapping [{enable | disable}]
ip multicast [vlan vid] proxying [enable | disable]
ip multicast helper-address [ip-address]
ipv6 multicast [vlan vid] admin-state [{enable | disable}]
ipv6 multicast [vlan vid] querier-forwarding [{enable | disable}]
no ipv6 multicast [vlan vid] querier-forwarding
ipv6 multicast [vlan vid] version [version]
ipv6 multicast max-group [num] [action {none | drop | replace}]
ipv6 multicast vlan vid max-group [num] [action {none | drop | replace}]
ipv6 multicast port slot | port max-group [num] [action {none | drop | replace}]
ipv6 multicast static-neighbor vlan vid {port slot/port | linkagg linkagg}
no ipv6 multicast static-neighbor vlan vid {port slot/port | linkagg linkagg}
ipv6 multicast static-querier vlan vid {port slot/port | linkagg linkagg}
no ipv6 multicast static-querier vlan vid {port slot/port | linkagg linkagg}
ipv6 multicast static-group ip_address vlan vid {port slot/port | linkagg linkagg}
no ipv6 multicast static-group ip_address vlan vid {port slot/port | linkagg linkagg}
ipv6 multicast [vlan vid] query-interval [seconds]
ipv6 multicast [vlan vid] last-member-query-interval [milliseconds]
ipv6 multicast [vlan vid] query-response-interval [milliseconds]
ipv6 multicast [vlan vid] unsolicited-report-interval [seconds]
ipv6 multicast [vlan vid] router-timeout [seconds]
ipv6 multicast [vlan vid] source-timeout [seconds]
ipv6 multicast [vlan vid] querying [{enable | disable}]
no ipv6 multicast [vlan vid] querying
ipv6 multicast [vlan vid] robustness [robustness]
ipv6 multicast [vlan vid] spoofing [{enable | disable}]
no ipv6 multicast [vlan vid] spoofing
ipv6 multicast [vlan vid] zapping [{enable | disable}]
ipv6 multicast [vlan vid] proxying [enable | disable]
show ip multicast [vlan vid]
show ip multicast port [slot/port]
show ip multicast forward [ip_address]
show ip multicast neighbor
show ip multicast querier
show ip multicast group [ip_address]
show ip multicast source [ip_address]
show ip multicast tunnel [address]
show ipv6 multicast [vlan vid]
show ipv6 multicast port [slot/port]
show ipv6 multicast forward [ipv6_address]
show ipv6 multicast neighbor
show ipv6 multicast querier
show ipv6 multicast group [ip_address]

```

```

show ipv6 multicast source [ip_address]
show ipv6 multicast tunnel [address]

```

DVMRP Commands

```

ip load dvmrp
ip dvmrp admin-state {enable | disable}
ip dvmrp flash-interval seconds
ip dvmrp graft-timeout seconds
ip dvmrp interface {interface_name}
no ip dvmrp interface {interface_name}
ip dvmrp interface {interface_name} metric value
ip dvmrp neighbor-interval seconds
ip dvmrp neighbor-timeout seconds
ip dvmrp prune-lifetime seconds
ip dvmrp prune-timeout seconds
ip dvmrp report-interval seconds
ip dvmrp route-holddown seconds
ip dvmrp route-timeout seconds
ip dvmrp subord-default {true | false}
ip interface name tunnel [source ip_address] [destination ip_address] [protocol {ipip | gre}]
no ip dvmrp interface name
show ip dvmrp
show ip dvmrp interface [ip_address | interface_name | enabled | disabled]
show ip dvmrp neighbor [ip_address]
show ip dvmrp nexthop [ip_address ip_mask]
show ip dvmrp prune [group_address source_address source_mask]
show ip dvmrp route [ip_address ip_mask]
show ip dvmrp tunnel [local_address remote_address]

```

PIM Commands

```

ip load pim
ip pim sparse admin-state {enable | disable}
ip pim dense admin-state {enable | disable}
ip pim static-rp group_address/prefix_length rp_address [[no] override] [priority priority]
ip pim rp-threshold bps
ip pim max-rps number
ip pim probe-time seconds
ip pim register checksum {header | full}
ip pim register-suppress-timeout seconds
ip pim spt admin-state {enable | disable}
ip pim state-refresh-interval seconds
ip pim state-refresh- limit ticks

```

```

ip pim state-refresh- ttl num
show ip pim sparse
show ip pim dense
show ip pim neighbor [ip_address]
show ip pim candidate-rp
show ip pim group-map [bsr | static-rp | ssm | dense]
show ip pim interface [if_name]
show ip pim static-rp
ipv6 pim sparse admin-state {enable | disable}
ipv6 pim static-rp group_address/prefix_length rp_address [[no] override] [priority priority]
ipv6 pim spt admin-state {enable | disable}
show ipv6 pim neighbor [ipv6_address] [if_name]

```

Multicast Routing Commands

```

ip mroute-boundary if_name scoped_address mask
no ip mroute-boundary if_name scoped_address mask
ip mroute interface if_name ttl threshold
show ip mroute-boundary
show ip mroute
show ip mroute interface {interface_name}
show ipv6 mroute interface {interface_name}
show ip mroute-nexthop

```

QoS Commands

```

qos {enable | disable}
qos trust-ports
qos no trust-ports
qos forward log
qos no forward log
qos log console
qos no log console
qos log lines lines
qos log level level
qos no log level
qos stats interval seconds
qos phones [priority priority_value | trusted]
qos no phones
qos user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmp | pim | isis | dhcp-
server | dns-reply}
qos no user-port {filter | shutdown}
qos dei {ingress | egress}
qos no dei {ingress | egress}

```

```

debug qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3]
[classifier] [nat] [sem] [pm] [ingress] [egress]
debug no qos
debug no qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2]
[l3] [classifier] [nat] [sem] [pm] [ingress] [egress]
debug qos internal [slice slot/slice] [flow] [queue] [port] [l2tree] [l3tree] [vector] [pending]
[verbose] [mapper] [pool] [log] [pingonly | nopingonly]
clear qos log
qos apply
qos revert
qos flush
qos reset
qos stats reset
qos port slot/port reset
qos port slot/port[-port]
qos port slot/port[-port] trusted
qos port slot/port no trusted
qos port slot/port[-port] maximum egress-bandwidth bps[k | m | g | t]
qos port slot/port[-port] no maximum egress-bandwidth
qos port slot/port[-port] maximum ingress-bandwidth bps[k | m | g | t]
qos port slot/port[-port] no maximum ingress-bandwidth
qos port slot/port[-port] maximum depth bps[k | m | g | t]
qos port slot/port[-port] no maximum depth
qos port slot/port[-port] default 802.1p value
qos port slot/port[-port] default dscp value
qos port slot/port[-port] default classification {tos | 802.1p | dscp}
qos port slot/port dei {ingress | egress}
qos port slot/port no dei {ingress | egress}
qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} qsp {qsp_id | qsp_name}
qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} wred admin-state {enable |
disable}
qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} stats {admin-state {enable
| disable} | interval interval_time}}
show qos port [slot/port] [statistics]
show qos slice [slot/slice]
show qos log
show qos config
show qos statistics
show qos wrp [wrp_id | wrp_name] [detail [port slot/port[-port]] | slot slot | linkagg agg_id[-
agg_id]]
show qos qsp [qsp_id | qsp_name] [detail [port slot/port[-port]] | slot slot | linkagg agg_id[-
agg_id]]
show qos qsi [port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]] [detail]

```

```

show qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} [qi-id qi_id | qi qi_id]
stats
show qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} [qi qi_id] stats rate
[bytes]
show qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} [qi qi_id] stats bytes
show qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} wred-stats [rate |
bytes]
clear qos qsi {port slot/port[-port] | slot slot | linkagg agg_id[-agg_id]} [qi-id qi_id] stats
qos qsp dcb {dcp_id | dcp_name} import qsp dcb {import_dcp_id | import_dcp_name}
[802.3x-pause]
no qos qsp dcb {dcp_id | dcp_name}
qos qsp dcb {dcp_id | dcp_name} tc tc_num
{
pfc flow-type { ll | nll } |
pfc link-delay allowance |
min-bw % |
max-bw % |
recommended bw %
}
qos qsp dcb {dcp_id | dcp_name} tc-numbering tc_num
show qos qsp dcb [dcp_id | dcp_name] [tc tc_num]
qos qsi {port slot/port[-port] | linkagg agg[-agg]} dcb dcbx admin-state {enable | disable}
qos qsi {port slot/port[-port] | linkagg agg[-agg]} qsp dcb {dcp_id | dcb_name}
show qos qsi [port slot/port[-port2] | linkagg agg_id[-agg_id2]] dcb dcbx [status]
show qos qsi {port slot/port[-port] | linkagg agg_id[-agg_id]} summary
qos qsi {port slot/port[-port2] | linkagg agg[-agg2]} dcb dcbx ets [config-tlv {enable | disable}
| recommend-tlv {enable | disable} | willing {yes | no}]
show qos qsi {port slot/port[-port] | linkagg agg[-agg]} dcb ets [tc [tc_num]]
qos qsi {port slot/port[-port] | linkagg agg[-agg]} dcb dcbx pfc [config-tlv {enable | disable}
| defense {enable | disable} | willing {yes | no}]
show qos qsi {port slot/port[-port] | linkagg agg[-agg]} dcb pfc
show qos pfc-lossless-usage
show qos qsi [port slot/port[-port]] dcb pfc stats
qos qsi {port chassis/slot/port[-port]} stats {admin-state {enable | disable} | interval minutes}
show qos qsi [port chassis/slot/port[-port]] stats [bytes] [packets]
clear qos qsi {port slot/port[-port]} dcb pfc stats

```

QoS Policy Commands

```

policy rule rule_name [enable | disable] [precedence precedence] [condition condition]
[action action] [validity-period name] [save] [log [log-interval seconds]] [count {packets
| bytes}] [trap] [default-list]
policy rule rule_name no {validity-period | save | log | trap | default-list}
no policy rule rule_name

```

```

policy validity-period name [days days] [months months] [hours hh:mm to hh:mm] [interval
mm:dd:yyyy hh:mm to mm:dd:yyyy hh:mm]
policy validity-period name no {hours / interval}
no policy validity-period name
policy list list_name type unp [enable | disable]
no policy list list_name
policy list list_name rules rule_name [rule_name2...]
policy list list_name no rules rule_name [rule_name2...]
policy network group net_group ip_address [mask net_mask] [ip_address2 [mask
net_mask2]...]
no policy network group net_group
policy network group net_group no ip_address [mask netmask] [ip_address2 [mask
net_mask2]...]
policy service group service_group service_name1 [service_name2...]
no policy service group service_group
policy service group service_group no service_name1 [service_name2...]
policy mac group mac_group mac_address [mask mac_mask] [mac_address2 [mask
mac_mask2]...]
no policy mac group mac_group
policy mac group mac_group no mac_address [mask mac_mask] [mac_address2 [mask
mac_mask2]...]
policy port group group_name slot/port[-port] [slot/port[-port]...]
no policy port group group_name
policy port group group_name no slot/port[-port] [slot/port[-port]...]
policy map group map_group {value1:value2...}
no policy map group map_group
policy map group no {value1:value2...}
policy service service_name
no policy service service_name
policy service service_name protocol protocol {[source ip-port port[-port]]
[destination ip-port port[-port]]}
no policy service service_name
policy service service_name no {source ip-port | destination ip-port}
policy service service_name source tcp-port port[-port]
no policy service service_name
policy service service_name no source tcp port
policy service service_name destination tcp-port port[-port]
no policy service service_name
policy service service_name no destination tcp-port
policy service service_name source udp-port port[-port]
no policy service service_name
policy service service_name no source udp-port
policy service service_name destination udp-port port[-port]
no policy service service_name

```

policy service *service_name* no destination udp-port
 policy condition *condition_name*
 no policy condition *condition_name*
 policy condition *condition_name* source ip *ip_address* [mask *netmask*]
 policy condition *condition_name* no source ip
 policy condition *condition_name* source ipv6 {any | *ipv6_address* [mask *netmask*]}
 policy condition *condition_name* no source ipv6
 policy condition *condition_name* destination ip *ip_address* [mask *netmask*]
 policy condition *condition_name* no destination ip
 policy condition *condition_name* destination ipv6 {any | *ipv6_address* [mask *netmask*]}
 policy condition *condition_name* no destination ipv6
 policy condition *condition_name* multicast ip *ip_address* [mask *netmask*]
 policy condition *condition_name* no multicast ip
 policy condition *condition_name* source network group *network_group*
 policy condition *condition_name* no source network group
 policy condition *condition_name* destination network group *network_group*
 policy condition *condition_name* no destination network group
 policy condition *condition_name* multicast network group *multicast_group*
 policy condition *condition_name* no multicast network group
 policy condition *condition_name* source ip-port *port[-port]*
 policy condition *condition_name* no source ip-port
 policy condition *condition_name* destination ip-port *port[-port]*
 policy condition *condition_name* no destination ip-port
 policy condition *condition_name* source tcp-port *port[-port]*
 policy condition *condition_name* no source tcp-port
 policy condition *condition_name* destination tcp-port *port[-port]*
 policy condition *condition_name* no destination tcp-port
 policy condition *condition_name* source udp-port *port[-port]*
 policy condition *condition_name* no source udp-port
 policy condition *condition_name* destination udp-port *port[-port]*
 policy condition *condition_name* no destination udp-port
 policy condition *condition_name* ethertype *etype*
 policy condition *condition_name* no ethertype
 policy condition *condition_name* established
 policy condition *condition_name* no established
 policy condition *condition_name* tcpflags [any | all] {F | S | R | P | A | U | E | W} mask {F | S
 | R | P | A | U | E | W}
 policy condition *condition_name* no tcpflags
 policy condition *condition_name* service *service_name*
 policy condition *condition_name* no service
 policy condition *condition_name* service group *service_group*
 policy condition *condition_name* no service group
 policy condition *condition_name* icmptype *type*
 policy condition *condition_name* no icmptype

policy condition *condition_name* icmpcode *code*
 policy condition *condition_name* no icmpcode
 policy condition *condition_name* ip-protocol *protocol*
 policy condition *condition_name* no ip-protocol
 policy condition *condition_name* ipv6
 policy condition *condition_name* no ipv6
 policy condition *condition_name* nh *next_header_value*
 policy condition *condition_name* no nh
 policy condition *condition_name* flow-label *flow_label_value*
 policy condition *condition_name* no flow-label
 policy condition *condition_name* tos *tos_value* [mask *tos_mask*]
 policy condition *conditioning* no tos
 policy condition *condition_name* dscp {*dscp_value[-value]*} [mask *dscp_mask*]
 policy condition *condition_name* no dscp
 policy condition *condition_name* source mac *mac_address* [mask *mac_mask*]
 policy condition *condition_name* no source mac
 policy condition *condition_name* destination mac *mac_address* [mask *mac_mask*]
 policy condition *condition_name* no destination mac
 policy condition *condition_name* source mac group *group_name*
 policy condition *condition_name* no source mac group
 policy condition *condition_name* destination mac group *mac_group*
 policy condition *condition_name* no destination
 policy condition *condition_name* source vlan *vlan_id*
 policy condition *condition_name* no source vlan
 policy condition *condition_name* inner source-vlan *vlan_id*
 policy condition *condition_name* no inner source-vlan
 policy condition *condition_name* destination vlan *vlan_id*
 policy condition *condition_name* no destination vlan
 policy condition *condition_name* 802.1p *802.1p_value*
 policy condition *condition_name* no 802.1p
 policy condition *condition_name* inner 802.1p *802.1p_value*
 policy condition *condition_name* no inner 802.1p
 policy condition *condition_name* source port *slot/port[-port]*
 policy condition *condition_name* no source port
 policy condition *condition_name* destination port *slot/port[-port]*
 policy condition *condition_name* no destination port
 policy condition *condition_name* source port group *group_name*
 policy condition *condition_name* no source port group
 policy condition *condition_name* destination port group *group_name*
 policy condition *condition_name* no destination port
 policy condition *condition_name* vrf {*vrf_name* / **default**}
 policy condition *condition_name* no vrf
 policy condition *condition_name* fragments
 policy condition *condition_name* no fragments

policy action *action_name*
 policy no action *action_name*
 policy action *action_name* disposition {accept | drop | deny}
 policy action *action_name* no disposition
 policy action *action_name* shared
 policy action *action_name* no shared
 policy action *action_name* priority *priority_value*
 policy action *action_name* no priority
 policy action *action_name* maximum bandwidth *bps*[**k** | **m** | **g** | **t**]
 policy action *action_name* no maximum bandwidth
 policy action *action_name* maximum depth *bps*[**k** | **m** | **g** | **t**]
 policy action *action_name* no maximum depth
 policy action *action_name* cir *bps* [cbs **bps**] [pir *bps*] [pbs **bps**] [color-only]
 policy action *action_name* no cir
 policy action *action_name* no pir
 policy action *action_name* cpu priority *priority*
 policy action *action_name* no cpu priority
 policy action *action_name* tos *tos_value*
 policy action *action_name* no tos
 policy action *action_name* 802.1p *802.1p_value*
 policy action *action_name* no 802.1p
 policy action *action_name* dscp *dscp_value*
 policy action *action_name* no dscp
 policy action map {802.1p | tos | dscp} to {802.1p | tos| dscp} using *map_group*
 policy action no map
 policy action *action_name* permanent gateway-ip *ip_address*
 policy action *action_name* no permanent gateway-ip
 policy action *action_name* port-disable
 policy action *action_name* no port-disable
 policy action *action_name* redirect port *slot/port*
 policy action *action_name* no redirect port
 policy action *action_name* redirect linkagg *link_agg*
 policy action *action_name* no redirect linkagg
 policy action *action_name* no-cache
 policy action *action_name* no no-cache
 policy action *action_name* [ingress | egress | ingress egress] mirror *slot/port*
 policy action *action_name* no mirror *slot/port*
 show [applied] policy network group [*network_group*]
 show [applied] policy service [*service_name*]
 show [applied] policy service group [*service_group*]
 show [applied] policy mac group [*mac_group*]
 show [applied] policy port group [*group_name*]
 show [applied] policy map group [*group_name*]
 show [applied] policy action [*action_name*]

show [applied] policy condition [*condition_name*]
 show active [bridged | routed | multicast] policy rule [*rule_name*]
 show [applied] [bridged | routed | multicast] policy rule [*rule_name*]
 show policy validity period [*name*]
 show active policy list [*list_name*]
 show [applied] policy list [*list_name*]

Policy Server Commands

policy server load
 policy server flush
 policy server *ip_address* [port *port_number*] [admin-state {enable | disable}] [preference
 preference] [user *user_name* password *password*] [searchbase *search_string*] [ssl | no
 ssl]
 no policy server *ip_address* [port *port_number*]
 show policy server
 show policy server long
 show policy server statistics
 show policy server rules
 show policy server events

AAA Commands

aaa radius-server *server* [host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*]] [key
 secret] [retransmit *retries*] [timeout *seconds*] [auth-port *auth_port*] [acct-port *acct_port*]
 [vrf-name *name*]
 no aaa radius-server *server*
 aaa tacacs+-server *server* [host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*]} [key
 secret]
 [timeout *seconds*] [port *port*] [vrf-name *name*]
 no aaa tacacs+-server *server*
 aaa ldap-server *server_name* [host {*hostname* | *ip_address*} [*hostname2* | *ip_address2*]] [dn
 dn_name] [password *super_password*] [base *search_base*] [retransmit *retries*] [timeout
 seconds] [ssl | no ssl] [port *port*] [vrf-name *name*]
 no aaa ldap-server *server_name*
 aaa authentication {console | telnet | ftp | http | snmp | ssh | default} *server1* [*server2*...] [local]
 no aaa authentication [console | telnet | ftp | http | snmp | ssh | default]
 aaa authentication {console | telnet | ftp | http | snmp | ssh} default
 aaa accounting session *server1* [*server2*...] [local]
 no accounting session
 aaa accounting command *server1* [*server2*...] [local]
 no accounting command
 aaa device-authentication mac *server1* [*server2*] [*server3*] [*server4*]
 no device-authentication mac


```

user username [password password] [expiration {day | date}] [read-only | read-write
[families... / domains...] all | none]] [no snmp | no auth | sha | md5 | sha+des | md5+des]
[console-only {enable | disable}]
no user username
password
user password-size min size
user password-expiration {day / disable}
user password-policy cannot-contain-username {enable | disable}
user password-policy min-uppercase number
user password-policy min-uppercase number
user password-policy min-digit number
user password-policy min-nonalpha number
user password-history number
user password-min-age days
user lockout-window minutes
user lockout-threshold number
user lockout-duration minutes
user username {lockout | unlock}
show aaa server [server_name]
show aaa authentication
show aaa device-authentication
show aaa accounting
show user [username]
show user password-policy
show user lockout-setting
show aaa priv hexa [domain or family]

```

UNP Commands

```

unp vlan-profile unp_name vlan vlan_id [qos-policy-list list_name]
no unp vlan-profile unp_name
unp {port {slot/port[-port2] | linkagg agg_id}
no unp {port slot/port[-port2] | linkagg agg_id}
unp {port slot/port1[-port2] | linkagg agg_id} default-vlan-profile unp_name
no unp {port slot/port1[-port2] | linkagg agg_id} default-vlan-profile
unp {port slot/port1[-port2] | linkagg agg_id} mac-authentication {enable | disable}
unp {port slot/port1[-port2] | linkagg agg_id} mac-authentication pass-alternate vlan-profile
unp_name
no unp {port slot/port1[-port2] | linkagg agg_id} mac-authentication pass-alternate
unp {port slot/port1[-port2] | linkagg agg_id} classification {enable | disable}
unp port {port slot/port1[-port2] | linkagg agg_id} trust-tag {enable | disable}
no unp classification mac-range low_mac_address high_mac_address
unp classification vlan-tag vlan_id [tag-position {inner | outer}] {vlan-profile unp_name
no unp classification vlan-tag vlan_id

```

```

unp dynamic-vlan-configuration {enable | disable}
unp dynamic-profile-configuration {enable | disable}
unp auth-server-down-unp unp_name
no auth-server-down unp
show unp [unp_name | sync | out-of-sync | local]
show unp global configuration
show unp user [mac_address] [slot/port[-port2] | linkagg agg_id] [count]

```

Edge Virtual Bridging Commands

```

evb {port slot/port | linkagg linkagg_id} type vlan-bridging
no evb {port slot/port | linkagg linkagg_id}
Enables or disables manual operating configuration for OmniSwitch after obtaining the EVB
TLV setting.
evb evb-lldp manual {enable | disable}
evb ecp default-ack-timer ack_timer
evb ecp default-max-retry max-try
evb vdp default-resource-wait-delay delay
evb vdp default-keep-alive-timeout ka_timeout
show evb [port slot/port | linkagg linkagg_id]
show evb config
show evb sbp-config [ slot/port | linkagg linkagg_id ]
show evb cdcp-status [slot/port]
show evb s-channel [slot/port]
show evb ecp-status [slot/port]

```

Port Mapping Commands

```

port-mapping port_mapping_sessionid {enable | disable}
no port-mapping port_mapping_sessionid
port-mapping session_id unknown-unicast-flooding {enable | disable}
show port-mapping [port_mapping_sessionid]

```

Learned Port Security Commands

```

port-security {port slot/port[-port2] | chassis} admin-state {enable | disable | locked}
no port-security port slot/port[-port2]
port-security shutdown minutes [convert-to-static {enable | disable}] [no-aging {enable |
disable}] [boot-up {enable | disable}]
no port-security learning-window
port-security {port slot/port[-port2] / chassis} convert-to-static
port-security {port slot/port[-port2]} maximum number
port-security {port slot/port[-port2]} learn-trap-threshold number
port-security port slot/port[-port2] max-filtering number

```

```

port-security {port slot/port[-port2]} mac-range [low mac_address / high mac_address]
port-security port slot/port[-port2] violation {shutdown | restrict | discard}
show port-security {port [slot/port[-port2]] / slot slot}
show port-security brief
show port-security learning-window

```

Port Mirroring and Monitoring Commands

```

port-mirroring port_mirror_sessionid source {slot/port[-port2] [slot/port[-port2]...]
destination slot/port [rpmir-vlan vlan_id] [bidirectional | inport | outport] [unblocked
vlan_id]
[enable | disable]
port-mirroring port_mirror_sessionid no source {slot/port[-port2] [slot/port[-port2]...]
port-mirroring port_mirror_sessionid {enable | disable}
no port-mirroring port_mirror_sessionid
port-monitoring port_monitor_sessionid source slot/port
[{no file | file filename [size filesize] | [overwrite {on | off}]]}
[inport | outport | bidirectional] [timeout seconds] [enable | disable] [capture-type {full |
brief}]
port-monitoring port_monitor_sessionid {disable | pause | resume}
no port-monitoring port_monitor_sessionid
show port-mirroring status [port_mirror_sessionid]
show port-monitoring status [port_monitor_sessionid]
show port-monitoring file port_monitor_sessionid

```

sFlow Commands

```

sflow agent ip <ip_address>
no sflow agent ip <ip_address>
sflow receiver receiver_index {name string | timeout { seconds | forever} | address
{ip_address | ipv6address} | udp-port port | packet-size size Version num | release}
sflow sampler num port slot/port[-port] {receiver receiver_index | rate value | sample-hdr-size
size}
no sflow sampler num portlist
sflow poller num port slot/port[-port] {receiver receiver_index | interval value}
no sflow poller num portlist
show sflow agent
show sflow receiver [num]
show sflow sampler[num]
show sflow poller [num]

```

RMON Commands

```

rmon probes {stats | history | alarm} [entry-number] {enable | disable}

```

```

show rmon probes [stats | history | alarm] [entry-number]
show rmon events [event-number]

```

Switch Logging Commands

```

swlog {[enable | disable] | remote command-log {enable| disable} | preamble | hash-time-limit
num | duplicate-detect | console level num}
no swlog
swlog appid {all | string} {[library {all | string} | subapp {all | num}]} {[disable | enable | level
{level | num}] [vrf num]}
swlog output {tty {enable | disable} | console | flash | socket ip_address [vrf-name name]}
no swlog output {console | flash | socket ip_address}
swlog output flash-file-size kilobytes
swlog clear
show log swlog
show log swlog [timestamp mm/dd/yyyy hh:mm:ss] [slot num]
show swlog [library | appid {all | string}]

```

Health Monitoring Commands

```

health threshold {rx percent | txrx percent | memory percent | cpu percent }
health interval seconds
show health configuration
show health [port slot/port | slot slot [-slot1]] [statistics]
show health all {memory | cpu | rx | txrx}

```

Ethernet OAM Commands

```

ethoam vlan {vlanid-list} primary-vlan {vlan-id}
no ethoam vlan {vlanid-list}
ethoam domain name format {none | dnsname | mac-address-uint | string}
level num
no ethoam domain name
ethoam domain name mhf {none / explicit / default}
ethoam domain name id-permission {none | chassisid}
ethoam association ma_name format {vpnid | unsignedint | string | primaryvid | icc-based}
domain md_name primary-vlan vlan-id
no ethoam association ma_name domain md_name
ethoam association ma_name domain md_name mhf {none | default |
explicit | defer}
ethoam association ma_name domain md_name md_name id-permission
{none | chassisid | defer}

```

ethoam association *association_name* **domain** {*domain_name* | *mac_address*}
ccm-interval {**interval-invalid** | **interval100ms** | **interval1s** / **interval10s** / **interval1m** / **interval10m**}
ethoam association *ma_name* domain {*md_name* | *mac_add*}
endpoint-list *mep_id*[-*mep_id2*]
no ethoam association *association_name* domain {*domain_name* | *mac_add*}
endpoint-list *mep_id*[-*mep_id2*]
clear ethoam statistics [domain domain association association endpoint mep-id]
ethoam default-domain level {*num*}
no ethoam default-domain
ethoam default-domain mhf {none | default | explicit}
no ethoam default-domain
ethoam default-domain id-permission {none | chassisid}
no ethoam default-domain
ethoam default-domain primary-vlan {vlan-id} [level {**no-level** | num}] [mhf {none | default | explicit | defer}] [id-permission {none | chassisid | defer}]
no ethoam default-domain
ethoam endpoint *mep-id* domain *md_name* association *ma_name* direction { up | down } {port {*slot/port* | virtual | linkagg *agg_id*} [primary-vlan *vlan_id*]}
no ethoam endpoint mep-id domain *md_name* association *ma_name*
ethoam endpoint *mep_id* domain {*md_name* | *mac_address*} association *ma_name* admin-state {enable | disable}
ethoam endpoint *mep_id* domain {*md_name* | *mac_address*} association *ma_name* rfp {enable | disable}
ethoam endpoint *mep_id* domain {*md_name* | *mac_address*} association *ma_name* ccm {enable | disable}
ethoam endpoint *mep_id* domain {*md_name* | *mac_address*} association *ma_name* priority *ccm_ltm_priority*
ethoam endpoint *mep_id* domain {*md_name* | *mac_address*} association *ma_name* lowest-priority-defect *lowest_priority_defect*
ethoam linktrace {**target-macaddress** *mac_address* | **target-endpoint** *t-mepid*}
source-endpoint *s-mepid* **domain** {*d-name* | *mac_add*} **association** *a-name* [**flag** {**fdb-mpdb** | **fdbonly**}] [**hop-count** *hop_count*]
ethoam loopback {target-endpoint t-mepid | target-macaddress mac_add} source-endpoint s-mepid domain d-name association a-name [number num] [data string] [vlan-priority vlan-priority] [drop-eligible { true | false }]
ethoam fault-alarm-time *centiseconds* **endpoint** *endpoint_id* **domain** {*md_name* | *mac_address*}
association *ma_name*
no ethoam fault-alarm-time endpoint *endpoint_id* **domain** {*md_name* | *mac_address*}
association *ma_name*
ethoam fault-reset-time *centiseconds* **endpoint** *endpoint_id* **domain** {*mac_add* | *d-name*} **association** *a-name*

no ethoam fault-reset-time endpoint *endpoint_id* **domain** {*mac_add* | *d-name*} **association** *a-name*
ethoam one-way-delay {target-endpoint t-mepid | target-macaddress mac_add} source-endpoint s-mepid domain domain association association [vlan- priority vlan-priority]
ethoam two-way-delay {target-endpoint t-mepid | target-macaddress mac_add} source-endpoint s-mepid domain domain association association [vlan- priority vlan-priority]
clear ethoam {one-way-delay-table | two-way-delay-table}
show ethoam
show ethoam domain *md_name*
show ethoam domain *md_name* **association** *ma_name*
show ethoam domain *md_name* **association** *ma_name* **end-point** *mep-id*
show ethoam default-domain configuration
show ethoam default-domain [**primary-vlan** *vlan_id*]
show ethoam remote-endpoint domain *d_name* **association** *a_name* **end-point** *s-mepid* [**remote-mep** *r-mepid*]
show ethoam cfmstack {**port** *slot/port* | virtual | **linkagg** *agg_num*}
show ethoam linktrace-reply domain *d-name* **association** *a-name* **endpoint** *s-mepid* **tran-id** *num*
show ethoam linktrace-tran-id domain {*domain_name* | *mac_address*} **association** *association_name* **endpoint** *mep_id*
show ethoam vlan vlan-id
show ethoam statistics domain {*domain_name* | *mac_address*} [**association** *association_name*] [**end-point** *endpoint_id*]
show ethoam config-error [vlan *vlan_id*] [{*port slot/port* | linkagg *agg_id*}]
show ethoam one-way-delay domain domain association association endpoint *s-mepid* [*mac-address mac-add*]
show ethoam two-way-delay domain domain association association endpoint *s-mepid* [*mac-address mac-add*]

Service Assurance Agent Commands

saa string [*descr description*] [*interval interval*]
no *saa string*
saa string type ip-ping destination-ip ipv4 addr source-ip ipv4 addr type-of-service tos [num-pkts count] [inter-pkt-delay delay] [payload-size size]
saa string type mac-ping destination-mac mac vlan vlan-id [vlan-priority vlan-priority] [drop-eligible {true | false}] [data data] [num-pkts count] [inter-pkt-delay delay] [payload-size size] [isid-check isid]
saa string type ethoam-loopback {target-endpoint tmep_id | target-mac address mac} source-endpoint smep_id domain domain association assoc vlan-priority priority [drop-eligible {true | false}] [data data] [num-pkts num] [inter-pkt-delay delay]
saa string type {ethoam-two-way-delay} {target-endpoint tmep_id | target-mac address mac} source-endpoint smep_id domain domain association assoc vlan-priority priority [num-pkts num] [inter-pkt-delay delay]

```

saa string start [at yyyy-mm-dd,hh:mm:ss.ds]
saa string stop [never | at yyyy-mm-dd,hh:mm:ss.ds]
show saa [string | {descr description}]
show saa [string] type {mac-ping | ip-ping | ethoam-loopback | ethoam-two-way-delay}
config
show saa [string] statistics [aggregate | history]

```

VLAN Stacking Commands

```

ethernet-service svlan {svlan_id [-svlan_id2]} [admin-state {enable | disable}] [stp {enable |
disable}] [name description]

```

```

no ethernet-service svlan {svlan_id [-svlan_id2]}

```

```

ethernet-service svlan svlan1[-svlan2] source-learning {enable| disable}

```

Creates a VLAN Stacking service and associates the service with an SVLAN. A service can be carried only on a single SVLAN. All traffic within the associated service is carried on the SVLAN.

```

ethernet-service service-name service-name svlan svlan_id

```

```

no ethernet-service service-name service-name svlan svlan_id

```

```

ethernet-service nni {port slot/port [-port2]} | linkagg linkagg_id [-linkagg_id2]} [tpid
tpid_value]

```

```

[[stp | mvrp] legacy-bpdu {enable | disable}]

```

```

no ethernet-service nni {port slot/port [-port2]} | linkagg linkagg_id [-linkagg_id2]}

```

```

ethernet-service svlan {svlan_id [-svlan_id2]} nni {port slot/port[-port2]} | linkagg linkagg_id
[-linkagg_id2]}

```

```

no ethernet-service svlan {svlan_id [-svlan_id2]} nni {port slot/port[-port2]} | linkagg
linkagg_id
[-linkagg_id2]}

```

```

ethernet-service sap sap_id service-name service_name

```

```

no ethernet-service sap sap_id

```

```

ethernet-service sap {sap_id} uni {port slot/port[-port2]} | linkagg linkagg_id [-
linkagg_id2]}

```

```

no ethernet-service sap {sap_id} uni {port slot/port[-port2]} | linkagg linkagg_id [-
linkagg_id2]}

```

```

ethernet-service sap {sap_id} cvlan {all | cvlan_id | cvlan_id1-cvlan_id2 / untagged}

```

```

no ethernet-service sap {sap_id} cvlan {all | cvlan_id | cvlan_id1-cvlan_id2 / untagged}

```

```

ethernet-service sap-profile sap_profile_name [bandwidth not-assigned] [[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][egress-bandwidth mbps]

```

```

no ethernet-service sap-profile sap_profile_name

```

```

ethernet-service sap sap_id sap-profile sap_profile_name

```

```

no ethernet-service sap sap_id

```

```

ethernet-service uni-profile uni-profile-name [l2-protocol {stp | 802.1x | 802.1ab | 802.3ad |
mvrp | amap} {peer | discard | tunnel}]

```

```

no ethernet-service uni-profile uni-profile-name

```

```

ethernet-service uni {port slot/port[-port2]} | linkagg linkagg_id [-linkagg_id2]} uni-profile
uni-profile-name

```

```

no ethernet-service uni-profile uni-profile-name

```

```

show ethernet-service vlan [svlan_id-[svlan_id2]]

```

```

show ethernet-service [service-name service-name / svlan svlan_id]

```

```

show ethernet-services sap [sap_id]

```

```

show ethernet-service port {slot/port / linkagg linkagg_id}

```

```

show ethernet-service nni [port slot/port / linkagg linkagg_id]

```

```

show ethernet-service uni [port slot/port / linkagg linkagg_id]

```

```

show ethernet-service uni-profile [uni-profile-name]

```

```

show ethernet-service sap-profile sap_profile_name

```

Service Manager Commands

```

service spb service_id isid instance_id bvlan bvlan_id

```

```

no service spb {service_id | all} [bvlan bvlan_id]

```

```

service spb service_id description desc_info

```

```

service spb service_id no description

```

```

service spb {service_id | all} stats {enable | disable}

```

```

service spb {service_id | all} admin-state {enable | disable}

```

```

service spb {service_id | all} multicast-mode {head-end | tandem}

```

```

service spb {service_id | all} vlan-xtation {enable | disable}

```

```

service spb {service_id | all} service-mtu bytes

```

```

service l2profile profile-name [stp | 802.1x | 802.1ab | 802.3ad | gvrp | mvrp | amap | pdu | vlan
| uplink] [peer | discard | tunnel]

```

```

no service l2profile profile-name

```

```

service access {port slot/port[-port2]} / linkagg agg_id[-agg_id2]

```

```

no service access {port slot/port[-port2]} / linkagg agg_id[-agg_id2]

```

```

service access {port slot/port[-port2]} / linkagg agg_id[-agg_id2] l2profile {default | profile-
name}

```

```

service access {port slot/port[-port2]} / linkagg agg_id[-agg_id2] vlan-xtation {enable |
disable}

```

```

service spb service_id sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag |
:outer_qtag.inner_qtag]

```

```

service spb service_id no sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag |
:outer_qtag.inner_qtag]

```

```

service spb service_id sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag |
:outer_qtag.inner_qtag] description desc_info

```

```

service spb service_id no sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag |
:outer_qtag.inner_qtag] no description

```

```

service spb service_id sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag |
:outer_qtag.inner_qtag] trusted

```

```

service spb service_id sap {port slot/port | linkagg agg_num} [:0 | :all | :qtag |
:outer_qtag.inner_qtag] no trusted priority value
service spb service_id sap {port slot/port | linkagg agg_id} [:0 | :all | :qtag |
:outer_qtag.inner_qtag] admin-state {enable | disable}
service spb service_id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1 |
:outer_qtag.inner_qtag] stats {enable | disable}
show service l2profile [profile_name]
show service access [port slot/port | linkagg agg_id]
show service [spb]
show service spb service_id ports
show service spb service_id sap {slot/port | linkagg agg_num} [:0 | :all | :qtag1 |
:outer_qtag.inner_qtag]
show service sdp [spb]
show service mesh-sdp [spb]
show service spb service_id ports
show service spb service_id [sap {port slot/port | linkagg agg_id][:0 | :all | :qtag |
:outer_qtag.inner_qtag] | mesh-sdp sdp_id] counters
clear service spb service_id [sap {port slot/port | linkagg agg_id][:0 | :all | :qtag |
:outer_qtag.inner_qtag] | mesh-sdp sdp_id] counters

```

CMM Commands

```

reload secondary [in [hours:] minutes | at hour:minute [month day / day month]]
reload secondary cancel
reload all [in [hours:] minutes | at hour:minute [month day / day month]]
reload all cancel
reload from image-dir {rollback-timeout minutes | no rollback-timeout [in [hours:] minutes |
at hour:minute] [redundancy-time minutes]}
reload slot slot
copy certified image-dir [make-running-directory]
issu from image-dir [redundancy-time minutes]
issu slot num
write memory [flash-synchro]
copy running certified [flash-synchro]
modify running-directory image-dir
copy flash-synchro
takeover
show running-directory
show reload [status | all status]
show microcode [certified | loaded | issu | image-dir]
usb {enable | disable}
usb auto-copy {enable | disable}
mount [/uflash]
umount /uflash

```

```

show usb statistics
show issu status

```

Chassis Management and Monitoring Commands

```

system contact text_string
system name text_string
system location text_string
system date [mm/dd/yyyy]
system time [hh:mm:ss]
system timezone [timezone_abbrev]
system daylight-savings-time
reload slot slot
power slot slot
no power slot slot
temp-threshold temp
powersupply enable [slot]
powersupply powersave {enable | disable}
hash-control {brief | extended [udp-tcp-port] | load-balance non-ucast {enable | disable}}
hash-control extended no udp-tcp-port
license apply file file_name
show system
show hardware info
show chassis
show cmm [slot]
show slot [slot]
show module [slot]
show module long [slot]
show module status [slot]
show powersupply [slot] [powersave status]
show fan [slot]
show fantray [slot]
show temperature [fabric [index] | slot [index] | fantray [index] | cmm [index | cmm_letter]]
show hash-control [non-ucast]
show license-info

```

Chassis MAC Server (CMS) Commands

```

mac-range eeprom start_mac_address count
show mac-range [index]
show mac-range [index] alloc

```

Network Time Protocol Commands

```
no ntp server {ip_address}
ntp server synchronized
ntp server unsynchronized
ntp client admin-state {enable | disable}
ntp src-ip preferred {default | no-loopback0 | ip_address}
no ntp src-ip preferred
ntp broadcast-client {enable | disable}
ntp broadcast-delay microseconds
ntp key key [trusted | untrusted]
ntp key load
ntp authenticate {enable | disable}
ntp master {stratum-number}
ntp interface {interface-ip} {enable | disable}
ntp max-associations {number}
ntp broadcast {broadcast-addr} [version version] [minpoll poll interval]
no ntp broadcast {broadcast-addr}
ntp peer {ip-address} [key keyid] [version version] [minpoll poll interval]
no ntp peer {ip-address}
ntp vrf-name name
show ntp status
show ntp client
show ntp client server-list
show ntp server client-list
show ntp server status [ip_address]
show ntp keys
```

Session Management Commands

```
session login-attempt integer
session login-timeout seconds
session {cli | ftp | http} banner file_name
no session {cli | ftp | http} banner
session {cli | http | ftp} timeout minutes
session prompt default [string]
session xon-xoff {enable | disable}
show prefix
user profile save
user profile reset
history number
!! | n
command-log {enable | disable}
kill session_number
```

```
exit
whoami
who
show session config
show session xon-xoff
more filename
[vrf name] telnet {port [default | service_port] | admin-state [enable | disable] | host_name | ip_address}
[vrf name] ssh {port [default | service_port] | admin-state [enable | disable] | host_name | ip_address}
ssh enforce-publickey-auth {enable | disable}
show command-log
show command-log status
[vrf name] show telnet
[vrf name] show ssh
```

File Management Commands

```
cd [path]
pwd
mkdir [options] [path] /dirname
rmdir [options] dirname
ls [options] [path/]filename
rm [options] [path/]filename
cp [options] source destination
scp [options] user_name@remote_ip_addr:[path/]source [path/]target
scp [options] [path/]source user_name@remote_ip_addr:[path/]target
mv [options] source destination
chmod {+w | -w} [path/]file
freespace [/flash | /uflash]
newfs /uflash
rcp [rem-slot: source_filepath destination_filepath]
rm filepath
rmdir directory [file_name]
vi [options] [path/]filename
tty lines columns
show tty
ftpt [options] host [port]
ftp {port [default | service_port] | admin-state [enable | disable] | host_name | ip_address}
[vrf name] ftp admin-state [enable | disable]
[vrf name] show ftp
```

Web Management Commands

```
[vrf name] webview server enable
[vrf name] webview server disable
[vrf name] webview access enable
[vrf name] webview access disable
webview force-ssl enable
webview force-ssl disable
webview http-port {default | port port}
webview https-port {default | port port}
[vrf name] show webview
```

Configuration File Manager Commands

```
configuration apply filename [at hh:mm month dd [year]] | [in hh[:mm]] [verbose]
configuration error-file-limit number
show configuration status
configuration cancel
configuration syntax-check path/filename [verbose]
configuration snapshot feature_list [path/filename]
show configuration snapshot [feature_list]
write terminal
```

SNMP Commands

```
snmp station {ip_address | ipv6_address} {[udp_port] [username] [v1 | v2 | v3] [enable |
disable]}
no snmp station {ip_address | ipv6_address}
show snmp station
snmp community-map community_string {[user useraccount_name] | {enable | disable}}
no snmp community-map community_string
snmp community-map mode {enable | disable}
show snmp community-map
snmp security {no-security | authentication set | authentication all | privacy set | privacy all |
trap-only}
show snmp security
show snmp statistics
show snmp mib-family [table_name]
snmp-trap absorption {enable | disable}
snmp-trap to-webview {enable | disable}
snmp-trap replay-ip {ip_address | ipv6_address} [seq_id]
snmp-trap filter-ip {ip_address | ipv6_address} trap_id_list
no snmp-trap filter-ip {ip_address | ipv6_address} trap_id_list
snmp authentication-trap {enable | disable}
```

```
show snmp-trap replay-ip
show snmp-trap filter-ip
show snmp authentication-trap
show snmp-trap config
```

DNS Commands

```
ip domain-lookup
no ip domain-lookup
ip name-server server-address1 [server-address2 [server-address3]]
ipv6 name-server server-ipv6_address1 [server-ipv6_address2 [server-ipv6_address3]]
ip domain-name name
no ip domain-name
show dns
```


Index

Numerics

- 802.1ab 12-1
 - notification of local system MIB changes 12-9
 - reinit delay 12-5
 - show port statistics 12-21, 12-35
 - tlv management 12-11
 - transmit time interval 12-2
- 802.1p
 - mapped to ToS or DSCP 29-144
 - QoS port default 28-42
- 802.1Q
 - untrusted ports 28-5

A

- AAA 31-1
 - password-size min 31-26
 - show user network profile 32-17, 32-21, 32-37, 32-41, 32-44
- accounting 1-33
- actions
 - supported by hardware 29-123
- active login sessions 49-22
- alerts 39-4
- assigning ports to VLANs 4-4

B

- BGP 22-1
 - aggregate routes 22-32
 - autonomous system 22-8
 - communities 22-38, 22-50
 - confederation 22-24
 - fast external failover 22-15
 - load 22-6
 - local preference 22-13
 - MED 22-53, 22-207
 - neighbor 22-55, 22-212, 22-216
 - policy 22-96
 - route dampening 22-28
 - route reflectors 22-19
- boot.cfg file
 - QoS log lines 28-9
- BPDU
 - see* Bridge Protocol Data Units
- Bridge Protocol Data Units 6-3, 6-55, 6-57, 6-59, 6-61

C

- CCM
 - priority value 41-33
 - transmission interval 41-15

- transmission rate 41-31
- CLI
 - logging commands 49-17, 49-33–49-35
- CMM
 - running configuration 45-9
 - takeover 45-17
- CMS 47-1
 - allocated addresses 47-6
 - mac-range 47-2
 - range table 47-4
- conditions
 - multiple conditions defined 29-40
- Continuity Check Messages
 - see* CCM
- current user session 49-20

D

- Data Center Bridging 28-2
- DCB
 - see* Data Center Bridging
- debug messages 39-4
- default route
 - IP 13-12
- DHCP Relay 18-1
 - DHCP server IP address 18-2
 - elapsed boot time 18-9
 - forward delay time 18-9
 - Global DHCP 18-2
 - ip helper pre-support 18-17
 - maximum number of hops 18-11
 - per-VLAN forwarding option 18-7
 - show ip helper 18-26
 - standard forwarding option 18-6
 - statistics 18-28
- directory
 - change 50-2
 - create 50-4
 - delete 50-6
 - display 50-3, 50-8, 50-19, 50-21, 50-25
- DNS
 - domain name 54-2
 - enables resolver 54-2
 - name servers 54-2, 54-3, 54-7, 54-9
 - resolver 54-1
- DSCP
 - mapped to 802.1p or ToS 29-144
 - QoS port default 28-44
- DVMRP
 - interface 25-6
 - neighbor 25-8
 - status 25-3
 - tunnel 25-17
- dynamic link aggregation
 - adding ports 8-29
 - creating 8-11, 9-10
 - deleting 8-11, 9-10
 - deleting ports 8-29
 - LACPDU frames 8-32, 8-38

- local port MAC address 8-34
 - remote group MAC address 8-23
 - remote port MAC address 8-40
- E**
- Edge Virtual Bridging 33-1
 - editor
 - vi 50-27
 - error file 52-4
 - error frame 1-38
 - errors 39-4
 - Ethernet 1-1
 - flow 1-3
 - interfaces 1-5
 - trap port 1-3
 - ethernet domain 41-5, 41-50, 41-53
 - Ethernet OAM 41-1
 - association endpoint list 41-17
 - lowest priority fault alarm 41-25, 41-35
 - maintenance association 41-9
 - EVB
 - see* Edge Virtual Bridging
 - exit 49-19
- F**
- Fadvrout.img file 26-5, 26-6
 - fault alarm
 - alarm time 41-41
 - reset time 41-43
 - file
 - copy 50-12, 50-14, 50-23
 - delete 50-10, 50-22, 50-24
 - move 50-16
 - privileges 50-18
 - system check 50-19, 50-20
 - transfer 50-32, 50-36
- G**
- GVRP 11-1
 - applicant 11-8
 - disable on specified port 11-2
 - display configuration on specified port 11-28, 11-31, 11-42
 - enable on specified port 11-2
 - registration 11-7
 - timer 11-10, 11-24
- H**
- health 40-2
 - high availability VLANs
 - egress ports 5-2, 5-4, 5-5, 5-6, 5-7, 5-8, 5-10
- I**
- IGMP
 - default 24-7, 24-87, 24-90
 - group entry 24-19, 24-93, 24-99
 - ip multicast querier-forwarding 24-5
 - last member query interval 24-23, 24-87, 24-90
 - neighbor entry 24-15, 24-94
 - querier entry 24-17, 24-96
 - query interval 24-21, 24-87, 24-90
 - query response interval 24-25, 24-27, 24-87, 24-90
 - querying 24-5, 24-33, 24-87, 24-90
 - robustness variable 24-35, 24-87, 24-90
 - router timeout 24-29, 24-87, 24-90
 - source timeout 24-31, 24-87, 24-90
 - spoofing 24-37, 24-87, 24-90
 - zapping 24-39, 24-41, 24-87, 24-90
 - interior gateway protocol
 - OSPF 20-1, 21-1
 - IP
 - interface tunnel 13-8, 25-17
 - IP Multicast Switching
 - see* IPMS 24-1
 - IP routing
 - default route 13-12
 - IPMS 24-1
 - ipv6 multicast querier-forwarding 24-46
 - ipv6
 - address 14-8
 - dad-check 14-13
 - hop-limit 14-14
 - interface 14-3
 - interface tunnel source destination 14-10
 - neighbor 14-16, 14-17
 - ping6 14-25
 - pmtu-lifetime 14-14, 14-15
 - prefix 14-19
 - rip 14-71
 - route 14-21
 - traceroute 14-28
- L**
- LACP
 - see* dynamic link aggregation
 - Link Trace Messages 41-37
 - priority value 41-33
 - link-state protocol
 - OSPF 20-1, 21-1
 - LPS 35-1
 - learning-window 35-4
 - learn-trap-threshold 35-11
 - max-filtering 35-13
 - maximum 35-9
- M**
- MAC address table
 - duplicate MAC addresses 3-8
 - MAC address VLAN rule 32-17, 32-19, 32-21
 - MAC addresses
 - aging time 3-11
 - dynamic link aggregation 8-23, 8-34, 8-40
 - statically assigned 3-7, 3-10
 - Maintenance Association

- create 41-9
 - modify 41-17
 - Maintenance Intermediate Point
 - see* MIP
 - Management Domain
 - display all information 41-4, 41-6, 41-7, 41-8, 41-50, 41-53, 42-4, 42-6, 42-8, 42-11, 42-14, 42-16, 42-18, 42-20, 42-28
 - display specific information 41-6, 41-8, 41-52, 42-4, 42-6, 42-8, 42-11, 42-14, 42-16, 42-18
 - MEP
 - administrative state 41-17, 41-27
 - MHF value 41-7
 - MLD
 - default 24-48, 24-107, 24-110
 - group entry 24-60, 24-112, 24-118, 24-120
 - last member query interval 24-64, 24-107, 24-110
 - neighbor entry 24-56, 24-113
 - querier entry 24-58, 24-115
 - query interval 24-62, 24-107, 24-110
 - query response interval 24-66, 24-68, 24-107, 24-110
 - querying 24-74, 24-107, 24-110
 - robustness variable 24-76, 24-107, 24-110
 - router timeout 24-70, 24-107, 24-110
 - source timeout 24-72, 24-107, 24-110
 - spoofing 24-78, 24-107, 24-110
 - zapping 24-80, 24-82, 24-107, 24-110
 - mobile ports
 - trusted ports 28-5
 - modules
 - power 46-14
 - reloading 45-4
 - temperature 46-15, 46-18
 - multicast routing
 - show routing information 27-11
 - multicast address boundaries 27-7
 - multicast routing
 - boundary 27-3
 - datagram ttl threshold 27-6
 - interface ttl 27-5, 27-6
 - ipv6 next-hop information 27-19
- N**
- Network Interface (NI) modules
 - reloading 46-11, 46-12, 46-13
 - NTP 48-1
 - broadcast delay 48-11, 48-20
 - key 48-12
 - operation 48-7
 - server 48-3, 48-17, 48-19, 48-21
 - server unsynchronization 48-6
 - synchronization 48-5, 48-25
- O**
- OSPF
 - area 20-21
 - global 20-3
 - graceful restart 20-46
 - interface 20-27
 - link-state protocol 20-1, 21-1
- P**
- pending configuration
 - commands associated with 28-27
 - erasing policy configuration 28-27
 - pim
 - cbsr 26-11
 - ipv6 pim sgroute 26-122
 - ipv6 pim sparse mode 26-92
 - max-rps 26-20, 26-39, 26-93
 - neighbor loss notification period 26-32
 - probe-time 26-22, 26-39
 - register checksum 26-23, 26-39
 - register-suppress-timeout 26-24, 26-39, 26-93
 - rp-candidate 26-17
 - rp-threshold 26-17
 - show pim notifications 26-63
 - sparse status 26-5, 26-39, 26-41
 - spt status 26-25, 26-39, 26-88, 26-93
 - ssm group 26-7
 - static-rp 26-13
 - PIM-SM v2 26-23
 - PMM
 - port mirroring 36-2
 - port monitoring source 36-7
 - policies
 - save option 29-6
 - policy condition
 - dscp 29-93
 - source vlan 29-103
 - policy servers
 - displaying information about 30-6
 - SSL 30-4
 - port mapping 34-2
- Q**
- QOS
 - ip phone traffic 28-13
- R**
- resolver
 - see* DNS resolver
 - RIP
 - active peer 16-33
 - forced hold-down timer 16-16
 - garbage timer 16-24
 - global 16-2
 - hold-down timer 16-25
 - host-route 16-18
 - IGP 16-1
 - interface 16-4
 - invalid timer 16-23
 - route-tag 16-19
 - security 16-20
 - status 16-3

- RMON
 - probes 38-2
- S**
- secure shell session 49-30, 49-31, 50-35
- secure socket layer
 - see* SSL
- Server Load Balancing 23-1
 - adding clusters 23-4
 - adding servers 23-13
 - deleting clusters 23-4, 23-13
 - disabling 23-2
 - enabling 23-2
 - server administrative status 23-13
- Service Manager 44-1
- session management
 - banner 49-5
 - kills 49-18
 - login attempt 49-3
 - more 49-27
 - prompt 49-9
 - timeout 49-7
 - user profile 49-12
 - xon-xoff 49-10
- sflow 37-6
 - poller 37-8
 - receiver 37-3
 - sampler 37-6
- Shortest Path Bridging 7-1
 - backbone VLAN 7-3
 - services 44-1
- SLB
 - see* Server Load Balancing
- smurf attack 13-21
- snapshot 52-11
- SNMP
 - community map 53-7
 - community strings 53-7
 - security 53-11
 - station 53-3
 - statistics 53-15
 - trap 53-18
- source learning 3-1
 - MAC address table 3-1, 3-7, 3-10
- Spanning Tree Algorithm and Protocol 6-1
 - 1x1 operating mode 6-3, 6-8, 6-10, 6-13, 6-15, 6-109, 9-31
 - bridge ID 6-18
 - flat operating mode 6-3, 6-8, 6-10, 6-13, 6-15, 6-109, 9-31
 - path cost 6-39, 6-42, 6-45
 - port states 6-47, 6-49
 - pvst+ mode 6-30
- Spanning Tree port parameters
 - connection type 6-51, 6-52, 6-53, 6-54, 6-56, 6-58, 6-59, 6-62, 6-63, 6-64, 6-65, 6-66, 6-67, 6-68, 6-69, 6-70
 - link aggregate ports 6-34, 6-36
 - mode 6-47, 6-49
 - path cost 6-47, 6-49
 - Spanning Tree status 6-34, 6-36
- SPB
 - see* Shortest Path Bridging
- ssh6 49-32
- SSL 51-4
 - policy servers 30-4
- static link aggregation
 - creating 8-3, 8-52
 - deleting 8-3, 8-52
- static MAC addresses 3-7, 3-10
- syntax check 52-9
- system information
 - administrative contact 46-3
 - date 46-6
 - location 46-5
 - name 46-4
 - time 46-6, 46-7
 - time zone 46-8
- T**
- telnet 49-28
- timer session 52-6
- Time-To-Live
 - see* TTL
- ToS
 - mapped to 802.1p or DSCP 29-144
 - QoS port default 28-44
- TTL 27-5, 27-6
- U**
- UDLD 2-1
 - clear UDLD statistics 2-11
 - probe-message advertisement timer 2-7
 - show global status 2-12
 - show neighbor ports 2-18
- user accounts
 - SNMP access 31-22
- UTC 48-1
- V**
- VLAN rules
 - MAC address 32-17, 32-19, 32-21
- VLAN Stacking
 - display list of all or range of configured SVLANs 43-28, 43-32, 43-33, 43-45
 - ethernet-service sap 43-12
 - ethernet-service uni-profile 43-23
- VLANs 4-1, 4-2, 10-1
 - administrative status 4-2
 - default VLAN 4-4
 - description 4-2, 7-3
 - port assignments 4-4
 - secondary VLAN 4-4
 - Spanning Tree status 6-7

VRRP

- configure address 19-5
- configure/modify 19-3
- configuring priority 19-4
- delay 19-10
- display configuration 19-35
- display statistics 19-38
- display track-association 19-43
- display tracking policies 19-41
- enable/disable trap 19-9
- group 19-21
- preempt 19-15
- priority 19-13
- set 19-19
- show vrrp group-association 19-47
- track-association 19-8
- tracking policy 19-6

VRRP3

- configure address 19-32
- configure/modify 19-29
- display configuration 19-49
- display statistics 19-52
- display track-association 19-54
- enable/disable trap 19-33
- track-association 19-34

W

- warnings 39-4
- WebView
 - enabling/disabling 51-2, 51-3

