AT8402 CLI Reference Manual

AdvancedTCA

M5306_TECH_2 Manual ID
2.02 Revision Index
16 June, 2007 Date of Issue



Revision History

Publication Title:	AT8402 CLI Reference Manual	
ID Number:	M5306_TECH_2	
Rev. Index	**Brief Description of Changes**	**Date of Issue**
2.00	First Release for AT8402	12 Feb., 2007
2.01	Clock commands added	16 May, 2007
2.02	Remove BCM5650x references in chapter QoS, acl commands rework, change copy command parameter	16 June, 2007

Imprint

Kontron AG may be contacted via the following:

	North America	**EMEA**
	Kontron Canada, Inc.	Kontron Modular Computers GmbH
	616 Curé Boivin	Sudetenstrasse 7
	Boisbriand, Québec	87600 Kaufbeuren
	J7G 2A7 Canada	Germany
Tel:	(450) 437-5682	+49 (0) 8341 803 333
	(800) 354-4223	
Fax:	(450) 437-8053	+49 (0) 8341 803 339
E-mail:	support@ca.kontron.com	support-kom@kontron.com

For further information about Kontron AG, our products or services, please visit our Internet web site: www.kontron.com

Disclaimer

Copyright © 2006 Kontron AG. All rights reserved. All data is for information purposes only and not guaranteed for legal purposes. Information has been carefully checked and is believed to be accurate; however, no responsibility is assumed for inaccuracies. Kontron and the Kontron logo and all other trademarks or registered trademarks are the property of their respective owners and are recognized. Specifications are subject to change without notice.

Table of Content

Revision History ii
Imprint ii
Disclaimer ii
About This Book xvii
Why the Document was Created xvii
How to Use This Document xvii
Proprietary Note xvii
Trademarks xvii
Environmental Protection Statement xviii
Explanation of Symbols xviii
For Your Safety xviii
High Voltage Safety Instructions xix
Special Handling and Unpacking Instructions xix
General Instructions on Usage xix
Two Year Warranty xx

Chapter 1

1. Using the Command-Line Interface ..... 1 - 2
1.1 Command Syntax ..... 1 - 2
1.2 Command Conventions ..... 1 - 2
1.2.1 Common Parameter Values ..... 1 - 3
1.3 Slot/Port Naming Convention ..... 1 - 4
1.4 Using the “No” Form of a Command ..... 1 - 5
1.5 Command Modes ..... 1 - 5
1.5.1 Command Completion and Abbreviation ..... 1 - 7
1.5.2 CLI Error Messages ..... 1 - 8
1.5.3 CLI Line-Editing Conventions ..... 1 - 8
1.6 Using CLI Help ..... 1 - 9
1.7 Accessing the CLI ..... 1 - 9

Chapter 2

2. Switching Commands ....2 - 2
2.1 Port Configuration Commands ....2 - 2
2.1.1 interface ....2 - 2
2.1.2 auto-negotiate ....2 - 2
2.1.3 auto-negotiate all ....2 - 3
2.1.4 description ....2 - 3
2.1.5 mtu ....2 - 3
2.1.6 shutdown ....2 - 4
2.1.7 shutdown all ....2 - 4
2.1.8 speed ....2 - 4
2.1.9 speed all ....2 - 5
2.1.10 block ....2 - 5
2.1.11 show port ....2 - 5
2.1.12 show port protocol ....2 - 6
2.2 Spanning Tree Protocol (STP) Commands ....2 - 6
2.2.1 spanning-tree ....2 - 6
2.2.2 spanning-tree bpdumigrationcheck ....2 - 7
2.2.3 spanning-tree configuration name ....2 - 7
2.2.4 spanning-tree configuration revision ....2 - 7
2.2.5 spanning-tree edgeport ....2 - 8
2.2.6 spanning-tree forceversion ....2 - 8
2.2.7 spanning-tree forward-time ....2 - 8
2.2.8 spanning-tree hello-time ....2 - 9
2.2.9 spanning-tree max-age ....2 - 9
2.2.10 spanning-tree max-hops ....2 - 9
2.2.11 spanning-tree mst ....2 - 10
2.2.12 spanning-tree mst instance ....2 - 11
2.2.13 spanning-tree mst priority ....2 - 11
2.2.14 spanning-tree mst vlan ....2 - 12
2.2.15 spanning-tree port mode ....2 - 12
2.2.16 spanning-tree port mode all ....2 - 12
2.2.17 show spanning-tree ....2 - 13
2.2.18 show spanning-tree brief ....2 - 14
2.2.19 show spanning-tree interface ....2 - 14
2.2.20 show spanning-tree mst port detailed ....2 - 15
2.2.21 show spanning-tree mst port summary ....2 - 16
2.2.22 show spanning-tree mst summary ....2 - 16
2.2.23 show spanning-tree summary ....2 - 17
2.2.24 show spanning-tree vlan ....2 - 17
2.3 VLAN Commands ....2 - 17

2.3.1 vlan database ..... 2 - 17
2.3.2 network mgmt_vlan ..... 2 - 18
2.3.3 vlan ..... 2 - 18
2.3.4 vlan acceptframe ..... 2 - 18
2.3.5 vlan ingressfilter ..... 2 - 19
2.3.6 vlan makestatic ..... 2 - 19
2.3.7 vlan name ..... 2 - 19
2.3.8 vlan participation ..... 2 - 19
2.3.9 vlan participation all ..... 2 - 20
2.3.10 vlan port acceptframe all ..... 2 - 20
2.3.11 vlan port ingressfilter all ..... 2 - 21
2.3.12 vlan port pvid all ..... 2 - 21
2.3.13 vlan port tagging all ..... 2 - 21
2.3.14 vlan protocol group ..... 2 - 22
2.3.15 vlan protocol group add protocol ..... 2 - 22
2.3.16 vlan protocol group remove ..... 2 - 22
2.3.17 protocol group ..... 2 - 23
2.3.18 protocol vlan group ..... 2 - 23
2.3.19 protocol vlan group all ..... 2 - 23
2.3.20 vlan pvid ..... 2 - 24
2.3.21 vlan tagging ..... 2 - 24
2.3.22 vlan association subnet ..... 2 - 24
2.3.23 vlan association mac ..... 2 - 25
2.3.24 show vlan ..... 2 - 25
2.3.25 show vlan brief ..... 2 - 26
2.3.26 show vlan port ..... 2 - 26
2.3.27 show vlan association subnet ..... 2 - 27
2.3.28 show vlan association mac ..... 2 - 27
2.4 Double VLAN Commands ..... 2 - 28
2.4.1 dvlan-tunnel ethertype ..... 2 - 28
2.4.2 mode dot1q-tunnel ..... 2 - 28
2.4.3 mode dvlan-tunnel ..... 2 - 28
2.4.4 show dot1q-tunnel ..... 2 - 29
2.4.5 show dvlan-tunnel ..... 2 - 29
2.5 Provisioning (IEEE 802.1p) Commands ..... 2 - 29
2.5.1 vlan port priority all ..... 2 - 30
2.5.2 vlan priority ..... 2 - 30
2.6 Protected Ports Commands ..... 2 - 30
2.6.1 switchport protected (Global Config) ..... 2 - 30
2.6.2 switchport protected (Interface Config) ..... 2 - 31
2.6.3 show switchport protected ..... 2 - 31
2.6.4 show interfaces switchport ..... 2 - 31
2.7 GARP Commands ..... 2 - 32
2.7.1 set garp timer join ..... 2 - 32
2.7.2 set garp timer leave ..... 2 - 32

2.7.3 set garp timer leaveall ....2 - 33
2.7.4 show garp ....2 - 33
2.8 GVRP Commands ....2 - 34
2.8.1 set gvrp adminmode ....2 - 34
2.8.2 set gvrp interfacemode ....2 - 34
2.8.3 show gvrp configuration ....2 - 34
2.9 GMRP Commands ....2 - 35
2.9.1 set gmrp adminmode ....2 - 35
2.9.2 set gmrp interfacemode ....2 - 36
2.9.3 show gmrp configuration ....2 - 36
2.9.4 show mac-address-table gmrp ....2 - 37
2.10 Port-Based Network Access Control Commands ....2 - 37
2.10.1 authentication login ....2 - 37
2.10.2 clear dot1x statistics ....2 - 38
2.10.3 clear radius statistics ....2 - 38
2.10.4 dot1x defaultlogin ....2 - 39
2.10.5 dot1x initialize ....2 - 39
2.10.6 dot1x login ....2 - 39
2.10.7 dot1x max-req ....2 - 39
2.10.8 dot1x port-control ....2 - 40
2.10.9 dot1x port-control all ....2 - 40
2.10.10 dot1x re-authenticate ....2 - 40
2.10.11 dot1x re-authentication ....2 - 41
2.10.12 dot1x system-auth-control ....2 - 41
2.10.13 dot1x timeout ....2 - 41
2.10.14 dot1x user ....2 - 42
2.10.15 users defaultlogin ....2 - 42
2.10.16 users login ....2 - 43
2.10.17 show authentication ....2 - 43
2.10.18 show authentication users ....2 - 43
2.10.19 show dot1x ....2 - 43
2.10.20 show dot1x users ....2 - 46
2.10.21 show users authentication ....2 - 46
2.11 Storm-Control Commands ....2 - 46
2.11.1 storm-control broadcast ....2 - 46
2.11.2 storm-control broadcast level ....2 - 47
2.11.3 storm-control broadcast all ....2 - 47
2.11.4 storm-control broadcast all level ....2 - 47
2.11.5 storm-control multicast ....2 - 48
2.11.6 storm-control multicast level ....2 - 48
2.11.7 storm-control multicast all ....2 - 48
2.11.8 storm-control multicast all level ....2 - 49
2.11.9 storm-control unicast ....2 - 49
2.11.10 storm-control unicast level ....2 - 50
2.11.11 storm-control unicast all ....2 - 50

2.11.12 storm-control unicast all level ..... 2 - 50
2.11.13 storm-control flowcontrol ..... 2 - 51
2.11.14 show storm-control ..... 2 - 51
2.12 Port-Channel/LAG (802.3ad) Commands ..... 2 - 52
2.12.1 port-channel ..... 2 - 52
2.12.2 addport ..... 2 - 52
2.12.3 deleteport (Interface Config) ..... 2 - 53
2.12.4 deleteport (Global Config) ..... 2 - 53
2.12.5 port-channel static ..... 2 - 53
2.12.6 port lacpmode ..... 2 - 53
2.12.7 port lacpmode all ..... 2 - 54
2.12.8 port lacp timeout (Interface Config) ..... 2 - 54
2.12.9 port lacp timeout (Global Config) ..... 2 - 54
2.12.10 port-channel adminmode ..... 2 - 55
2.12.11 port-channel linktrap ..... 2 - 55
2.12.12 port-channel name ..... 2 - 55
2.12.13 show port-channel brief ..... 2 - 55
2.12.14 show port-channel ..... 2 - 56
2.13 Port Mirroring ..... 2 - 56
2.13.1 monitor session ..... 2 - 57
2.13.2 no monitor ..... 2 - 57
2.13.3 show monitor session ..... 2 - 57
2.14 Static MAC Filtering ..... 2 - 58
2.14.1 macfilter ..... 2 - 58
2.14.2 macfilter addsrc ..... 2 - 59
2.14.3 macfilter addsrc all ..... 2 - 59
2.14.4 show mac-address-table static ..... 2 - 59
2.14.5 show mac-address-table staticfiltering ..... 2 - 60
2.15 IGMP Snooping Configuration Commands ..... 2 - 60
2.15.1 set igmp ..... 2 - 60
2.15.2 set igmp interfacemode ..... 2 - 61
2.15.3 set igmp fast-leave ..... 2 - 61
2.15.4 set igmp groupmembership-interval ..... 2 - 62
2.15.5 set igmp maxresponse ..... 2 - 62
2.15.6 set igmp mcrtexpiretime ..... 2 - 63
2.15.7 set igmp mrouter ..... 2 - 63
2.15.8 set igmp mrouter interface ..... 2 - 64
2.15.9 show igmpsnooping ..... 2 - 64
2.15.10 show igmpsnooping mrouter interface ..... 2 - 65
2.15.11 show igmpsnooping mrouter vlan ..... 2 - 65
2.15.12 show mac-address-table igmpsnooping ..... 2 - 66
2.16 Port Security Commands ..... 2 - 66
2.16.1 port-security ..... 2 - 66
2.16.2 port-security max-dynamic ..... 2 - 67
2.16.3 port-security max-static ..... 2 - 67

2.16.4 port-security mac-address ....2 - 67
2.16.5 port-security mac-address move ....2 - 68
2.16.6 show port-security ....2 - 68
2.16.7 show port-security dynamic ....2 - 68
2.16.8 show port-security static ....2 - 68
2.16.9 show port-security violation ....2 - 68
2.17 LLDP (802.1AB) Commands ....2 - 69
2.17.1 lldp transmit ....2 - 69
2.17.2 lldp receive ....2 - 69
2.17.3 lldp timers ....2 - 69
2.17.4 lldp transmit-tlv ....2 - 70
2.17.5 lldp transmit-mgmt ....2 - 70
2.17.6 lldp notification ....2 - 70
2.17.7 lldp notification-interval ....2 - 71
2.17.8 clear lldp statistics ....2 - 71
2.17.9 clear lldp remote-data ....2 - 71
2.17.10 show lldp ....2 - 71
2.17.11 show lldp interface ....2 - 72
2.17.12 show lldp statistics ....2 - 72
2.17.13 show lldp remote-device ....2 - 73
2.17.14 show lldp remote-device detail ....2 - 73
2.17.15 show lldp local-device ....2 - 74
2.17.16 show lldp local-device detail ....2 - 74
2.18 Denial of Service Commands ....2 - 74
2.18.1 dos-control sipdip ....2 - 75
2.18.2 dos-control firstfrag ....2 - 75
2.18.3 dos-control tcpfrag ....2 - 76
2.18.4 dos-control tcpflag ....2 - 76
2.18.5 dos-control l4port ....2 - 76
2.18.6 dos-control icmp ....2 - 77
2.18.7 show dos-control ....2 - 77
2.19 MAC Database Commands ....2 - 77
2.19.1 bridge aging-time ....2 - 78
2.19.2 show forwardingdb agetime ....2 - 78
2.19.3 show mac-address-table multicast ....2 - 78
2.19.4 show mac-address-table stats ....2 - 79

Chapter 3

3. Quality of Service (QoS) Commands ....3 - 2
3.1 Class of Service (CoS) Commands ....3 - 2
3.1.1 classofservice dot1p-mapping ....3 - 2
3.1.2 classofservice ip-dscp-mapping ....3 - 3

3.1.3 classofservice trust ..... 3 - 3
3.1.4 cos-queue min-bandwidth ..... 3 - 3
3.1.5 cos-queue strict ..... 3 - 4
3.1.6 traffic-shape ..... 3 - 4
3.1.7 show classofservice dot1p-mapping ..... 3 - 4
3.1.8 show classofservice ip-precedence-mapping ..... 3 - 5
3.1.9 show classofservice ip-dscp-mapping ..... 3 - 5
3.1.10 show classofservice trust ..... 3 - 5
3.1.11 show interfaces cos-queue ..... 3 - 6
3.2 Differentiated Services (DiffServ) Commands ..... 3 - 6
3.2.1 diffserv ..... 3 - 7
3.3 DiffServ Class Commands ..... 3 - 7
3.3.1 class-map ..... 3 - 8
3.3.2 class-map rename ..... 3 - 8
3.3.3 match any ..... 3 - 8
3.3.4 match class-map ..... 3 - 9
3.3.5 match dstip ..... 3 - 9
3.3.6 match dstl4port ..... 3 - 9
3.3.7 match ip dscp ..... 3 - 10
3.3.8 match ip precedence ..... 3 - 10
3.3.9 match ip tos ..... 3 - 10
3.3.10 match protocol ..... 3 - 11
3.3.11 match srcip ..... 3 - 11
3.3.12 match srcl4port ..... 3 - 11
3.4 DiffServ Policy Commands ..... 3 - 12
3.4.1 assign-queue ..... 3 - 12
3.4.2 drop ..... 3 - 12
3.4.3 conform-color ..... 3 - 12
3.4.4 class ..... 3 - 13
3.4.5 mark cos ..... 3 - 13
3.4.6 mark ip-dscp ..... 3 - 13
3.4.7 mark ip-precedence ..... 3 - 14
3.4.8 police-simple ..... 3 - 14
3.4.9 policy-map ..... 3 - 14
3.4.10 policy-map rename ..... 3 - 15
3.5 DiffServ Service Commands ..... 3 - 15
3.5.1 service-policy ..... 3 - 15
3.6 DiffServ Show Commands ..... 3 - 16
3.6.1 show class-map ..... 3 - 16
3.6.2 show diffserv ..... 3 - 17
3.6.3 show policy-map ..... 3 - 17
3.6.4 show diffserv service ..... 3 - 19
3.6.5 show diffserv service brief ..... 3 - 19
3.6.6 show policy-map interface ..... 3 - 20
3.6.7 show service-policy ..... 3 - 20

3.7 MAC Access Control List (ACL) Commands .....3 - 20
3.7.1 mac access-list extended .....3 - 21
3.7.2 mac access-list extended rename .....3 - 21
3.7.3 {deny | permit} .....3 - 21
3.7.4 mac access-group .....3 - 22
3.7.5 show mac access-lists .....3 - 23
3.8 IP Access Control List (ACL) Commands .....3 - 23
3.8.1 access-list .....3 - 24
3.8.2 ip access-group .....3 - 25
3.8.3 acl-trapflags .....3 - 26
3.8.4 show ip access-lists .....3 - 26
3.8.5 show access-lists .....3 - 27

Chapter 4

4. Utility Commands .....4 - 2
4.1 Commands for update and startup Configuration .....4 - 2
4.1.1 download ipmifw .....4 - 2
4.1.2 download initrd .....4 - 2
4.1.3 download frudata .....4 - 2
4.1.4 download fwum .....4 - 3
4.1.5 download bootloader .....4 - 3
4.1.6 download amcipmifw .....4 - 3
4.1.7 startupslot .....4 - 3
4.1.8 startupslot activate .....4 - 3
4.1.9 show startupconfig .....4 - 4
4.2 ATCA commands .....4 - 4
4.2.1 set board sensor threshold .....4 - 4
4.2.2 set board ipmi-controller debug .....4 - 4
4.2.3 set board device-id .....4 - 4
4.2.4 set board fcap .....4 - 4
4.2.5 show atca ekeying .....4 - 5
4.2.6 ekeying (interface) .....4 - 5
4.2.7 set board bootcycle .....4 - 5
4.3 System Information and Statistics Commands .....4 - 5
4.3.1 show arp switch .....4 - 6
4.3.2 show eventlog .....4 - 6
4.3.3 show hardware .....4 - 6
4.3.4 show version .....4 - 6
4.3.5 show interface .....4 - 7
4.3.6 show interface ethernet .....4 - 8
4.3.7 show mac-addr-table .....4 - 15
4.3.8 show running-config .....4 - 16

4.3.9 show sysinfo ..... 4 - 16
4.3.10 show tech-support ..... 4 - 17
4.3.11 show boardinfo post-status ..... 4 - 17
4.3.12 show boardinfo sensors ..... 4 - 17
4.3.13 show boardinfo event-log ..... 4 - 17
4.3.14 show boardinfo update-status ..... 4 - 17
4.3.15 show boardinfo version ..... 4 - 18
4.3.16 show boardinfo address ..... 4 - 18
4.3.17 show boardinfo fru ..... 4 - 18
4.3.18 show boardinfo ipmidev ..... 4 - 18
4.3.19 show boardinfo led ..... 4 - 18
4.3.20 show boardinfo fcap ..... 4 - 19
4.3.21 show boardinfo amc connection ..... 4 - 19
4.3.22 show boardinfo amc fru ..... 4 - 19
4.3.23 show boardinfo amc ipmidev ..... 4 - 19
4.3.24 show boardinfo bootcycle ..... 4 - 19
4.4 Logging Commands ..... 4 - 19
4.4.1 logging buffered ..... 4 - 20
4.4.2 logging buffered wrap ..... 4 - 20
4.4.3 logging cli-command ..... 4 - 20
4.4.4 logging console ..... 4 - 20
4.4.5 logging host ..... 4 - 21
4.4.6 logging host remove ..... 4 - 21
4.4.7 logging port ..... 4 - 21
4.4.8 logging syslog ..... 4 - 22
4.4.9 show logging ..... 4 - 22
4.4.10 show logging buffered ..... 4 - 22
4.4.11 show logging hosts ..... 4 - 23
4.4.12 show logging traplogs ..... 4 - 23
4.4.13 clear board event-log ..... 4 - 23
4.4.14 show logging backtrace ..... 4 - 23
4.4.15 show logging diag-report ..... 4 - 23
4.5 System Utility and Clear Commands ..... 4 - 24
4.5.1 traceroute ..... 4 - 24
4.5.2 clear config ..... 4 - 24
4.5.3 clear counters ..... 4 - 24
4.5.4 clear igmpsnooping ..... 4 - 24
4.5.5 clear pass ..... 4 - 24
4.5.6 clear port-channel ..... 4 - 25
4.5.7 clear traplog ..... 4 - 25
4.5.8 clear vlan ..... 4 - 25
4.5.9 enable passwd ..... 4 - 25
4.5.10 logout ..... 4 - 25
4.5.11 set bootstopkey ..... 4 - 25
4.5.12 ping ..... 4 - 26
4.5.13 quit ..... 4 - 26

4.5.14 reload ....4 - 26
4.5.15 copy ....4 - 26
4.6 Keying for Advanced Features ....4 - 27
4.6.1 license advanced ....4 - 27
4.6.2 show key-features ....4 - 28
4.7 Simple Network Time Protocol (SNTP) Commands ....4 - 28
4.7.1 sntp broadcast client poll-interval ....4 - 28
4.7.2 sntp client mode ....4 - 28
4.7.3 sntp client port ....4 - 29
4.7.4 sntp unicast client poll-interval ....4 - 29
4.7.5 sntp unicast client poll-timeout ....4 - 29
4.7.6 sntp unicast client poll-retry ....4 - 30
4.7.7 sntp multicast client poll-interval ....4 - 30
4.7.8 sntp server ....4 - 30
4.7.9 show sntp ....4 - 30
4.7.10 show sntp client ....4 - 31
4.7.11 show sntp server ....4 - 31
4.8 DHCP Server Commands ....4 - 32
4.8.1 ip dhcp pool ....4 - 32
4.8.2 client-identifier ....4 - 32
4.8.3 client-name ....4 - 33
4.8.4 default-router ....4 - 33
4.8.5 dns-server ....4 - 33
4.8.6 hardware-address ....4 - 34
4.8.7 host ....4 - 34
4.8.8 lease ....4 - 34
4.8.9 network (DHCP Pool Config) ....4 - 35
4.8.10 bootfile ....4 - 35
4.8.11 domain-name ....4 - 35
4.8.12 netbios-name-server ....4 - 36
4.8.13 netbios-node-type ....4 - 36
4.8.14 next-server ....4 - 36
4.8.15 option ....4 - 37
4.8.16 ip dhcp excluded-address ....4 - 37
4.8.17 ip dhcp ping packets ....4 - 38
4.8.18 service dhcp ....4 - 38
4.8.19 ip dhcp bootp automatic ....4 - 38
4.8.20 ip dhcp conflict logging ....4 - 39
4.8.21 clear ip dhcp binding ....4 - 39
4.8.22 clear ip dhcp server statistics ....4 - 39
4.8.23 clear ip dhcp conflict ....4 - 39
4.8.24 show ip dhcp binding ....4 - 39
4.8.25 show ip dhcp global configuration ....4 - 40
4.8.26 show ip dhcp pool configuration ....4 - 40
4.8.27 show ip dhcp server statistics ....4 - 41

4.8.28 show ip dhcp conflict ..... 4 - 41
4.9 DHCP Filtering ..... 4 - 42
4.9.1 ip dhcp filtering ..... 4 - 42
4.9.2 ip dhcp filtering trust ..... 4 - 42
4.9.3 show ip dhcp filtering ..... 4 - 42
4.10 Serviceability Packet Tracing Commands ..... 4 - 43
4.10.1 debug console ..... 4 - 43
4.10.2 debug clear ..... 4 - 43
4.10.3 debug spanning-tree bpdu transmit ..... 4 - 43
4.10.4 debug spanning-tree bpdu receive ..... 4 - 44
4.10.5 debug spanning-tree bpdu ..... 4 - 45
4.10.6 debug igmpsnooping packet transmit ..... 4 - 45
4.10.7 debug igmpsnooping packet receive ..... 4 - 46
4.10.8 debug igmpsnooping packet ..... 4 - 47
4.10.9 debug ping packet ..... 4 - 47
4.10.10 debug rip packet ..... 4 - 48
4.10.11 debug ospf packet ..... 4 - 49
4.10.12 debug lacp packet ..... 4 - 50

Chapter 5

5. Management Commands ..... 5 - 2
5.1 Network Interface Commands ..... 5 - 2
5.1.1 enable (Privileged EXEC access) ..... 5 - 2
5.1.2 serviceport ip ..... 5 - 2
5.1.3 serviceport protocol ..... 5 - 3
5.1.4 network parms ..... 5 - 3
5.1.5 network protocol ..... 5 - 3
5.1.6 network mac-address ..... 5 - 3
5.1.7 network mac-type ..... 5 - 3
5.1.8 show network ..... 5 - 4
5.1.9 show serviceport ..... 5 - 4
5.2 Console Port Access Commands ..... 5 - 5
5.2.1 configuration ..... 5 - 5
5.2.2 lineconfig ..... 5 - 5
5.2.3 serial baudrate ..... 5 - 5
5.2.4 serial timeout ..... 5 - 6
5.2.5 show serial ..... 5 - 6
5.3 Telnet Commands ..... 5 - 6
5.3.1 ip telnet server enable ..... 5 - 6
5.3.2 telnet ..... 5 - 7
5.3.3 transport input telnet ..... 5 - 7
5.3.4 transport output telnet ..... 5 - 7

5.3.5 session-limit ....5 - 8
5.3.6 session-timeout ....5 - 8
5.3.7 telnetcon maxsessions ....5 - 8
5.3.8 telnetcon timeout ....5 - 9
5.3.9 disconnect ....5 - 9
5.3.10 show loginsession ....5 - 9
5.3.11 show telnet ....5 - 10
5.3.12 show telnetcon ....5 - 10
5.4 Secure Shell (SSH) Command ....5 - 10
5.4.1 ip ssh ....5 - 10
5.4.2 ip ssh protocol ....5 - 11
5.4.3 ip ssh server enable ....5 - 11
5.4.4 sshcon maxsessions ....5 - 11
5.4.5 sshcon timeout ....5 - 12
5.4.6 show ip ssh ....5 - 12
5.5 User Account Commands ....5 - 12
5.5.1 users name ....5 - 12
5.5.2 users passwd ....5 - 13
5.5.3 users snmpv3 accessmode ....5 - 13
5.5.4 users snmpv3 authentication ....5 - 14
5.5.5 users snmpv3 encryption ....5 - 14
5.5.6 show users ....5 - 15
5.6 SNMP Commands ....5 - 15
5.6.1 snmp-server ....5 - 15
5.6.2 snmp-server community ....5 - 16
5.6.3 snmp-server community ipaddr ....5 - 16
5.6.4 snmp-server community ipmask ....5 - 16
5.6.5 snmp-server community mode ....5 - 17
5.6.6 snmp-server community ro ....5 - 17
5.6.7 snmp-server community rw ....5 - 17
5.6.8 snmp-server enable traps violation ....5 - 18
5.6.9 snmp-server enable traps ....5 - 18
5.6.10 snmp-server enable traps bcaststorm ....5 - 18
5.6.11 snmp-server enable traps linkmode ....5 - 19
5.6.12 snmp-server enable traps multiusers ....5 - 19
5.6.13 snmp-server enable traps stpmode ....5 - 19
5.6.14 snmptrap ....5 - 20
5.6.15 snmptrap snmpversion ....5 - 20
5.6.16 snmptrap ipaddr ....5 - 20
5.6.17 snmptrap mode ....5 - 20
5.6.18 snmp trap link-status ....5 - 21
5.6.19 snmp trap link-status all ....5 - 21
5.6.20 show snmpcommunity ....5 - 21
5.6.21 show snmptrap ....5 - 22
5.6.22 show trapflags ....5 - 22

5.7 CLI Command Logging Command ..... 5 - 23
5.7.1 logging cli-command ..... 5 - 23
5.8 RADIUS Commands ..... 5 - 23
5.8.1 radius accounting mode ..... 5 - 24
5.8.2 radius server host ..... 5 - 24
5.8.3 radius server key ..... 5 - 25
5.8.4 radius server msgauth ..... 5 - 25
5.8.5 radius server primary ..... 5 - 25
5.8.6 radius server retransmit ..... 5 - 25
5.8.7 radius server timeout ..... 5 - 26
5.8.8 show radius ..... 5 - 26
5.8.9 show radius accounting ..... 5 - 27
5.8.10 show radius statistics ..... 5 - 28
5.9 TACACS+ Commands ..... 5 - 29
5.9.1 tacacs-server host ..... 5 - 29
5.9.2 tacacs-server key ..... 5 - 29
5.9.3 tacacs-server timeout ..... 5 - 30
5.9.4 key ..... 5 - 30
5.9.5 port ..... 5 - 30
5.9.6 priority ..... 5 - 30
5.9.7 timeout ..... 5 - 31
5.9.8 show tacacs ..... 5 - 31
5.10 Configuration Scripting Commands ..... 5 - 31
5.10.1 script apply ..... 5 - 32
5.10.2 script delete ..... 5 - 32
5.10.3 script list ..... 5 - 32
5.10.4 script show ..... 5 - 32
5.10.5 script validate ..... 5 - 32
5.11 Pre-login Banner and System Prompt Commands ..... 5 - 33
5.11.1 copy (pre-login banner) ..... 5 - 33
5.11.2 set prompt ..... 5 - 33
5.12 Watchdog Support Commands ..... 5 - 33
5.12.1 set watchdog ..... 5 - 33
5.12.2 show watchdog ..... 5 - 34
5.13 Diagnostics Commands ..... 5 - 34
5.13.1 diagnostics ..... 5 - 34
5.13.2 copy nvram: diag-report url ..... 5 - 34
5.14 PCI express Commands ..... 5 - 34
5.14.1 set board pcie upstream ..... 5 - 34
5.14.2 set board pcie hotplug ..... 5 - 35
5.14.3 set board pcie clock ..... 5 - 35
5.14.4 set board pcie mode ..... 5 - 35
5.14.5 show boardinfo pcie ..... 5 - 36
5.15 Storage Commands ..... 5 - 36

5.15.1 set board storage connect .....5 - 36
5.15.2 show boardinfo storage .....5 - 37
5.15.3 set board sasexp program .....5 - 37
5.15.4 show board sasexp program .....5 - 37
5.16 Clock Support Commands .....5 - 37
5.16.1 show boardinfo pll status .....5 - 37
5.16.2 show boardinfo pll config .....5 - 37
5.16.3 set board pll .....5 - 37
5.16.4 show boardinfo clock bpl .....5 - 38
5.16.5 show boardinfo clock amc .....5 - 38
5.16.6 show boardinfo clock map .....5 - 38
5.16.7 set board clock bpl .....5 - 38
5.16.8 set board clock map .....5 - 39

Appendix A

A. Getting Help ..... A - 2

Appendix B

B. List of Commands ..... B - 2

About This Book

This document describes configuration commands for FASTPATH® software. The commands can be accessed from the CLI.

Why the Document was Created

This document was created primarily for system administrators configuring and operating a system using FASTPATH software. It is intended to provide an understanding of the configuration options of FASTPATH software.

In addition, software engineers who will be integrating FASTPATH software into their router or switch product can benefit from a description of the configuration options.

It is assumed that the reader has an understanding of the FASTPATH software base and has read the appropriate specification for the relevant networking device platform. It is also assumed that the reader has a basic knowledge of Ethernet and networking concepts.

How to Use This Document

- Chapter 1 “” details the procedure to quickly become acquainted with the FASTPATH software.



Note

Refer to the release notes for the FASTPATH application level code. The release notes detail the platform specific functionality of the Switching, Routing, SNMP, Config, Management, and Bandwidth Provisioning packages. The suite of features supported by the FASTPATH packages are not available on all the platforms to which FASTPATH has been ported.

Proprietary Note

This document contains information proprietary to Kontron Modular Computers GmbH. It may not be copied or transmitted by any means, disclosed to others, or stored in any retrieval system or media without the prior written consent of Kontron Modular Computers GmbH or one of its authorized agents.

The information contained in this document is, to the best of our knowledge, entirely correct. However, Kontron Modular Computers GmbH cannot accept liability for any inaccuracies or the consequences thereof, or for any liability arising from the use or application of any circuit, product, or example shown in this document.

Kontron Modular Computers GmbH reserves the right to change, modify, or improve this document or the product described herein, as seen fit by Kontron Modular Computers GmbH without further notice.

Trademarks

© 2005 LVL7 Systems, Inc. All rights reserved. FASTPATH® and MasterDriver® are registered trademarks, and LVL7™ and the LVL7 logo are trademarks of LVL7 Systems, Inc. All other trademarks are the property of their respective owners.

Linux is a registered trademark of Linus Torvalds.

RedHat is a registered trademark of RedHat

Kontron Modular Computers GmbH and the Kontron Logo are trade marks owned by Kontron Modular Computers GmbH, Kaufbeuren (Germany). In addition, this document may include

names, company logos and trademarks, which are registered trademarks and, therefore, proprietary to their respective owners.

Environmental Protection Statement

This product has been manufactured to satisfy environmental protection requirements where possible. Many of the components used (structural parts, printed circuit boards, connectors, batteries, etc.) are capable of being recycled.

Final disposition of this product after its service life must be accomplished in accordance with applicable country, state, or local laws or regulations.

Explanation of Symbols



CE Conformity

This symbol indicates that the product described in this manual is in compliance with all applied CE standards. Please refer also to the section “Applied Standards” in this manual.



Caution, Electric Shock!

This symbol and title warn of hazards due to electrical shocks (> 60V) when touching products or parts of them. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.

Please refer also to the section “High Voltage Safety Instructions” on the following page.



Warning, ESD Sensitive Device!

This symbol and title inform that electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times.

Please read also the section “Special Handling and Unpacking Instructions” on the following page.



Warning!

This symbol and title emphasize points which, if not fully understood and taken into consideration by the reader, may endanger your health and/or result in damage to your material.



Note...

This symbol and title emphasize aspects the reader should read through carefully for his or her own advantage.

For Your Safety

Your new Kontron product was developed and tested carefully to provide all features necessary to ensure its compliance with electrical safety requirements. It was also designed for a long fault-free life. However, the life expectancy of your product can be drastically reduced by improper treatment during unpacking and installation. Therefore, in the interest of your own safety and of the correct operation of your new Kontron product, you are requested to conform with the following guidelines.

High Voltage Safety Instructions



Warning!

All operations on this device must be carried out by sufficiently skilled personnel only.



Caution, Electric Shock!

Indicates that you must enter a value in place of the brackets and text inside them. Before installing your new Kontron product into a system always ensure that your mains power is switched off. This applies also to the installation of piggybacks.

Serious electrical shock hazards can exist during all installation, repair and maintenance operations with this product. Therefore, always unplug the power cable and any other cables which provide external voltages before performing work.

Special Handling and Unpacking Instructions



ESD Sensitive Device!

Electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times.

Do not handle this product out of its protective enclosure while it is not used for operational purposes unless it is otherwise protected.

Whenever possible, unpack or pack this product only at EOS/ESD safe work stations. Where a safe work station is not guaranteed, it is important for the user to be electrically discharged before touching the product with his/her hands or tools. This is most easily done by touching a metal part of your system housing.

It is particularly important to observe standard anti-static precautions when changing piggybacks, ROM devices, jumper settings etc. If the product contains batteries for RTC or memory back-up, ensure that the board is not placed on conductive surfaces, including anti-static plastics or sponges. They can cause short circuits and damage the batteries or conductive circuits on the board.

General Instructions on Usage

In order to maintain Kontron's product warranty, this product must not be altered or modified in any way. Changes or modifications to the device, which are not explicitly approved by Kontron Modular Computers GmbH and described in this manual or received from Kontron's Technical Support as a special handling instruction, will void your warranty.

This device should only be installed in or connected to systems that fulfill all necessary technical and specific environmental requirements. This applies also to the operational temperature range of the specific board version, which must not be exceeded. If batteries are present their temperature restrictions must be taken into account.

In performing all necessary installation and application operations, please follow only the instructions supplied by the present manual.

Keep all the original packaging material for future storage or warranty shipments. If it is necessary to store or ship the board please re-pack it as nearly as possible in the manner in which it was delivered.

Special care is necessary when handling or unpacking the product. Please, consult the special handling and unpacking instruction on the previous page of this manual.

Two Year Warranty

Kontron Modular Computers GmbH grants the original purchaser of Kontron's products a two year limited hardware warranty as described in the following. However, no other warranties that may be granted or implied by anyone on behalf of Kontron are valid unless the consumer has the express written consent of Kontron Modular Computers GmbH.

Kontron Modular Computers GmbH warrants their own products, excluding software, to be free from manufacturing and material defects for a period of 24 consecutive months from the date of purchase. This warranty is not transferable nor extendible to cover any other users or long-term storage of the product. It does not cover products which have been modified, altered or repaired by any other party than Kontron Modular Computers GmbH or their authorized agents. Furthermore, any product which has been, or is suspected of being damaged as a result of negligence, improper use, incorrect handling, servicing or maintenance, or which has been damaged as a result of excessive current/voltage or temperature, or which has had its serial number(s), any other markings or parts thereof altered, defaced or removed will also be excluded from this warranty.

If the customer's eligibility for warranty has not been voided, in the event of any claim, he may return the product at the earliest possible convenience to the original place of purchase, together with a copy of the original document of purchase, a full description of the application the product is used on and a description of the defect. Pack the product in such a way as to ensure safe transportation (see our safety instructions).

Kontron provides for repair or replacement of any part, assembly or sub-assembly at their own discretion, or to refund the original cost of purchase, if appropriate. In the event of repair, refunding or replacement of any part, the ownership of the removed or replaced parts reverts to Kontron Modular Computers GmbH, and the remaining part of the original guarantee, or any new guarantee to cover the repaired or replaced items, will be transferred to cover the new or repaired items. Any extensions to the original guarantee are considered gestures of goodwill, and will be defined in the "Repair Report" issued by Kontron with the repaired or replaced item.

Kontron Modular Computers GmbH will not accept liability for any further claims resulting directly or indirectly from any warranty claim, other than the above specified repair, replacement or refunding. In particular, all claims for damage to any system or process in which the product was employed, or any loss incurred as a result of the product not functioning at any given time, are excluded. The extent of Kontron Modular Computers GmbH liability to the customer shall not exceed the original purchase price of the item for which the claim exists.

Kontron Modular Computers GmbH issues no warranty or representation, either explicit or implicit, with respect to its products' reliability, fitness, quality, marketability or ability to fulfil

any particular application or purpose. As a result, the products are sold “as is,” and the responsibility to ensure their suitability for any given task remains that of the purchaser. In no event will Kontron be liable for direct, indirect or consequential damages resulting from the use of our hardware or software products, or documentation, even if Kontron were advised of the possibility of such claims prior to the purchase of the product or during any period since the date of its purchase.

Please remember that no Kontron Modular Computers GmbH employee, dealer or agent is authorized to make any modification or addition to the above specified terms, either verbally or in any other form, written or electronically transmitted, without the company’s consent.



Chapter 1

Using the Command-Line Interface

1. Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

- 1.1 “Command Syntax” on page 1 - 2
- 1.2 “Command Conventions” on page 1 - 2
- 1.3 “Slot/Port Naming Convention” on page 1 - 4
- 1.4 “Using the “No” Form of a Command” on page 1 - 5
- 1.5 “Command Modes” on page 1 - 5
- 1.6 “Using CLI Help” on page 1 - 9
- 1.7 “Accessing the CLI” on page 1 - 9

1.1 Command Syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as **`show network`** or **`clear vlan`**, do not require parameters. Other commands, such as **`network parms`**, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the **`network parms`** command syntax:

Format **`network parms`** *`<ipaddr> <netmask> [gateway]`*

- **`network parms`** is the command name.
- *`<ipaddr>`* and *`<netmask>`* are parameters and represent required values that you must enter after you type the command keywords.
- *`[gateway]`* is an optional parameter, so you are not required to enter a value in place of the parameter.

The CLI Reference lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The **`show`** commands also contain a description of the information that the command shows.

1.2 Command Conventions

In this document, the command name is in **`bold`** font. Parameters are in *`italic font`*. You must replace the parameter name with an appropriate value, which might be a name or number. Parameters are order dependent.

The parameters for a command might include mandatory values, optional values, or keyword choices. Table 4.1 describes the conventions this document uses to distinguish between value types.

Table 4.1. Parameter Conventions

Symbol	Example	Description
<> angle brackets	<*value*>	Indicates that you must enter a value in place of the brackets and text inside them.
[] square brackets	*[value]*	Indicates an optional parameter that you can enter in place of the brackets and text inside them.
{} curly braces	*{choice1 | choice2}*	Indicates that you must select a parameter from the list of choices.
| Vertical bars	*choice1 | choice2*	Separates the mutually exclusive choices.
[{}] Braces within square brackets	*[{choice1 | choice2}]*	Indicates a choice within an optional element.

1.2.1 Common Parameter Values

Parameter values might be names (strings) or numbers.To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (““) are not valid user-defined strings. Table 4.2 describes common parameter values and value formatting.

Table 4.2. Parameter Descriptions

Parameter	Description
ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats: **a** (32 bits) **a.b** (8.24 bits) **a.b.c** (8.8.16 bits) **a.b.c.d** (8.8.8.8) In addition to these formats, the CLI accepts decimal, hexidecimal and octal formats through the following input formats (where *n* is any valid hexidecimal, octal or decimal number): **0xn** (CLI assumes hexidecimal format) **0n** (CLI assumes octal format with leading zeros) **n** (CLI assumes decimal format)
areaid	Enter area IDs in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same format as IP addresses but are distinct from IP addresses. You can use the IP network number of the sub-netted network for the area ID.
routerid	Enter the value of <routerid> in dotted-decimal notation, such as 0.0.0.1. A router ID of 0.0.0.0 is invalid.

Table 4.2. Parameter Descriptions

Parameter	Description
Interface or slot/port	Valid slot and port number separated by forward slashes. For example, 0/1 represents slot number 0 and port number 1.
Logical Interface	Represents a Logical slot and port number.. This is applicable in the case of a port-channel (LAG). You can use the logical slot/port to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

1.3 Slot/Port Naming Convention

FASTPATH software references physical entities such as cards and ports by using a slot/port naming convention. The FASTPATH software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Table 4.3. Type of Slots

Slot Type	Description
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces.
CPU slot numbers	The CPU slots immediately follow the logical slots.

The port identifies the specific physical port or logical interface being managed on a given slot.

Table 4.4. Type of Ports

Port Type	Description
Physical Ports	The physical ports for each slot are numbered sequentially starting from zero.
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions. VLAN routing interfaces are only used for routing functions. Loopback interfaces are logical interfaces that are always up. Tunnel interfaces are logical point-to-point links that carry encapsulated packets.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

NOTE: In the CLI, loopback and tunnel interfaces do not use the slot/port format. To specify a loopback interface, you use the loopback ID. To specify a tunnel interface, you use the tunnel ID.

1.4 Using the “No” Form of a Command

The **no** keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a **no** form. In general, use the **no** form to reverse the action of a command or reset a value back to the default. For example, the **no shutdown** configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Only the configuration commands are available in the **no** form.

1.5 Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific FASTPATH software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. Table 4.5 describes the command modes and the prompts visible in that mode.

Table 4.5. CLI Command Modes

Command Mode	Prompt	Mode Description
User EXEC	**Switch>**	Contains a limited set of commands to view basic system information.
Privileged EXEC	**Switch#**	Allows you to issue any **EXEC** command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	**Switch (Config)#**	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	**Switch (Vlan)#**	Groups all the VLAN commands.
Interface Config	**Switch (Interface <**slot/port**>)#** Switch (Interface Loopback <id>)# Switch (Interface Tunnel <id>)#	Allows you to enable or modify the operation of an interface and provides access to the router interface configuration commands. Use this mode to set up a physical port for a specific logical connection operation.

Table 4.5. CLI Command Modes

Command Mode	Prompt	Mode Description
Line Config	`Switch (line)#`	Allows you to configure various telnet settings and the console interface.
Policy Map Config	`Switch (Config-policy-map)#`	Allows you to access the QoS Policy-Map configuration mode to configure the QoS Policy-Map.
Policy Class Config	`Switch (Config-policy-class-map)#`	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	`Switch (Config-class-map)#`	Allows you to access the QoS Class-Map configuration mode to configure QoS class maps.
MAC Access-list Config	`Switch (Config-mac-access-list)#`	Allows you to create a MAC Access-List and to enter the mode containing Mac Access-List configuration commands.
TACACS Config	`Switch (Tacacs)#`	Allows you to configure properties for the TACACS servers.
DHCP Pool Config	`Switch (Config dhcp-pool)#`	Allows you to access the DHCP Pool configuration.

Table 4.6 explains how to enter or exit each mode.

Table 4.6. CLI Mode Access and Exit

Command Mode	Access Method	Exit or Access Previous Mode
User EXEC	This is the first level of access.	To exit, enter **`logout`**.
Privileged EXEC	From the User EXEC mode, enter **`enable`**.	To exit to the User EXEC mode, enter **`exit`** or press ***`Ctrl-Z`***.
Global Config	From the Privileged EXEC mode, enter **`configure`**.	To exit to the Privileged EXEC mode, enter **`exit`**, or press ***`Ctrl-Z`***.
VLAN Config	From the Privileged EXEC mode, enter **`vlan database`**.	To exit to the Privileged EXEC mode, enter **`exit`**, or press ***`Ctrl-Z`***.

Table 4.6. CLI Mode Access and Exit

Command Mode	Access Method	Exit or Access Previous Mode
Interface Config	From the Global Config mode, enter **interface** <slot/port> *or* **interface loopback** *<id>* or **interface tunnel** *<id>* or	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter ***Ctrl-Z***.
Line Config	From the Global Config mode, enter **lineconfig**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter ***Ctrl-Z***.
Policy-Map Config	From the Global Config mode, enter **policy-map**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter ***Ctrl-Z***.
Policy-Class-Map Config	From the Policy Map mode enter **class**.	To exit to the Policy Map mode, enter **exit**. To return to the Privileged EXEC mode, enter ***Ctrl-Z***.
Class-Map Config	From the Global Config mode, enter **class-map**.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter ***Ctrl-Z***.
MAC Access-list Config	From the Global Config mode, enter **mac access-list extended** *<name>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter ***Ctrl-Z***.
TACACS Config	From the Global Config mode, enter **tacacs-server host** *<ip-addr>*, where *<ip-addr>* is the IP address of the TACACS server on your network.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter ***Ctrl-Z***.
DHCP Pool Config	From the Global Config mode, enter **ip dhcp pool** *<pool-name>*.	To exit to the Global Config mode, enter **exit**. To return to the Privileged EXEC mode, enter ***Ctrl-Z***.

1.5.1 Command Completion and Abbreviation

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the SPACEBAR or TAB key to complete the word.

Command abbreviation allows you to execute a command when you have entered there are enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

1.5.2 CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 4.7 describes the most common CLI error messages.

Table 4.7. CLI Error Messages

Message Text	Description
`% Invalid input detected at '^' marker.`	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.
`Command not found / Incomplete command. Use ? to list commands.`	Indicates that you did not enter the required keywords or values.
`Ambiguous command`	Indicates that you did not enter enough letters to uniquely identify the command.

1.5.3 CLI Line-Editing Conventions

Table 4.8 describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering **`help`** from the User or Privileged EXEC modes.

Table 4.8. CLI Editing Conventions

Key Sequence	Description
DEL or Backspace	Delete previous character
Ctrl-A	Go to beginning of line
Ctrl-E	Go to end of line
Ctrl-F	Go forward one character
Ctrl-B	Go backward one character
Ctrl-D	Delete current character
Ctrl-U, X	Delete to beginning of line
Ctrl-K	Delete to end of line
Ctrl-W	Delete previous word
Ctrl-T	Transpose previous character
Ctrl-P	Go to previous line in history buffer
Ctrl-R	Rewrites or pastes the line
Ctrl-N	Go to next line in history buffer
Ctrl-Y	Prints last deleted character
Ctrl-Q	Enables serial flow
Ctrl-S	Disables serial flow
Ctrl-Z	Return to root command prompt
Tab, <SPACE>	Command-line completion
Exit	Go to next lower command prompt
?	List available commands, keywords, or parameters

1.6 Using CLI Help

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
(switch) >?

enable                    Enter into user privilege mode.
help                      Display help for various special keys.
logout                   Exit this session. Any unsaved changes are lost.
ping                      Send ICMP echo packets to a specified IP
address.
quit                     Exit this session. Any unsaved changes are lost.
show                      Display Switch Options and Settings.
telnet                    Telnet to a remote host.
```

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
(switch) #network ?

javamode                  Enable/Disable.
mgmt_vlan                Configure the Management VLAN ID of the switch.
parms                     Configure Network Parameters of the router.
protocol                  Select DHCP, BootP, or None as the network
config
                          protocol.
```

If the help output shows a parameter in angle brackets, you must replace the parameter with a value.

```
(switch) #network parms ?

<ipaddr>                  Enter the IP Address.
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>                      Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(switch) #show m?

mac-addr-table            mac-address-table        monitor
```

1.7 Accessing the CLI

You can access the CLI by using a direct console connection or by using a telnet or SSH connection from a remote management host.

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP or DHCP server on your network. For more information, see 5.1 “Network Interface Commands” on page 5 - 2.



Chapter 2

Switching Commands

2. Switching Commands

This chapter describes the switching commands available in the CLI.

The Switching Commands chapter includes the following sections:

- 2.1 “Port Configuration Commands” on page 2 - 2
- 2.2 “Spanning Tree Protocol (STP) Commands” on page 2 - 6
- 2.3 “VLAN Commands” on page 2 - 17
- 2.4 “Double VLAN Commands” on page 2 - 28
- 2.5 “Provisioning (IEEE 802.1p) Commands” on page 2 - 29
- 2.6 “Protected Ports Commands” on page 2 - 30
- 2.7 “GARP Commands” on page 2 - 32
- 2.8 “GVRP Commands” on page 2 - 34
- 2.9 “GMRP Commands” on page 2 - 35
- 2.10 “Port-Based Network Access Control Commands” on page 2 - 37
- 2.11 “Storm-Control Commands” on page 2 - 46
- 2.12 “Port-Channel/LAG (802.3ad) Commands” on page 2 - 52
- 2.13 “Port Mirroring” on page 2 - 56
- 2.15 “IGMP Snooping Configuration Commands” on page 2 - 60
- 2.16 “Port Security Commands” on page 2 - 66
- 2.17 “LLDP (802.1AB) Commands” on page 2 - 69
- 2.18 “Denial of Service Commands” on page 2 - 74
- 2.19 “MAC Database Commands” on page 2 - 77

CAUTION: The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

2.1 Port Configuration Commands

This section describes the commands you use to view and configure port settings.

2.1.1 interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port).

Format `interface` <slot/port>

Mode Global Config

2.1.2 auto-negotiate

This command enables automatic negotiation on a port.

Default enabled

Format `auto-negotiate`

Mode Interface Config

2.1.2.1 no auto-negotiate

This command disables automatic negotiation on a port.

NOTE: Automatic sensing is disabled when automatic negotiation is disabled.

Format `no auto-negotiate`

Mode Interface Config

2.1.3 auto-negotiate all

This command enables automatic negotiation on all ports.

Default enabled

Format `auto-negotiate all`

Mode Global Config

2.1.3.1 no auto-negotiate all

This command disables automatic negotiation on all ports.

Format `no auto-negotiate all`

Mode Global Config

2.1.4 description

Use this command to create an alpha-numeric description of the port.

Format `description` <*description*>

Mode Interface Config

2.1.5 mtu

Use the `mtu` command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the `mtu` command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard FASTPATH implementation, the MTU size is a valid integer between 1522 - 9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.

NOTE: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require.

Default 1518 (untagged)

Format `mtu` <*1518-9216*>

Mode Interface Config

2.1.5.1 no mtu

This command sets the default MTU size (in bytes) for the interface.

Format `no mtu`

Mode Interface Config

2.1.6 shutdown

This command disables a port.

NOTE: You can use the **shutdown** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default enabled

Format **shutdown**

Mode Interface Config

2.1.6.1 no shutdown

This command enables a port.

Format **no shutdown**

Mode Interface Config

2.1.7 shutdown all

This command disables all ports.

NOTE: You can use the **shutdown all** command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default enabled

Format **shutdown all**

Mode Global Config

2.1.7.1 no shutdown all

This command enables all ports.

Format **no shutdown all**

Mode Global Config

2.1.8 speed

This command sets the speed and duplex setting for the interface.

Format **speed** *{<100 | 10> <half-duplex | full-duplex>}*

Mode Interface Config

Acceptable values are:

100h 100BASE-T half duplex

100f 100BASE-T full duplex

10h 10BASE-T half duplex

10f 10BASE-T full duplex

2.1.9 speed all

This command sets the speed and duplex setting for all interfaces.

Format `speed all` *{<100 | 10> <half-duplex | full-duplex>}*

Mode Global Config

Acceptable values are:

100h 100BASE-T half-duplex

100f 100BASE-T full duplex

10h 10BASE-T half duplex

10f 10BASE-T full duplex

2.1.10 block

This command sets a port in blocking mode. A blocking port will not receive or forward data frames. The command is only allowed if no spanning tree is enabled because the spanning tree is setting the port states itself. If the port is currently disabled, the state is not changed until it will become enabled. The state of the ports can be listed (spanning tree) by using:

```
show spanning-tree mst port summary 0 all
```

Format `block`

Mode Interface Config

2.1.10.1 no block

This command resets a port in non-blocking mode.

Format `no block`

Mode Interface Config

2.1.11 show port

This command displays port information.

Format `show port` *{*<slot/port> | *all}*

Mode Privileged EXEC

Interface Valid slot and port number separated by forward slashes.

Type If not blank, this field indicates that this port is a special type of port. The possible values are:

Mirror - this port is a monitoring port. For more information, see 2.13 “Port Mirroring” on page 2 - 56.

PC Mbr- this port is a member of a port-channel (LAG).

Probe - this port is a probe port.

Admin Mode The Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled. The factory default is enabled.

Physical Mode The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.

Physical Status The port speed and duplex mode.

Link Status The Link is up or down.

Link Trap This object determines whether or not to send a trap when link status changes. The factory default is enabled.

LACP Mode LACP is enabled or disabled on this port.

2.1.12 show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format `show port protocol` *{<groupid> | all}*

Mode Privileged EXEC

Group Name The group name of an entry in the Protocol-based VLAN table.

Group ID The group identifier of the protocol group.

Protocol(s) The type of protocol(s) for this group.

VLAN The VLAN associated with this Protocol Group.

Interface(s) Lists the slot/port interface(s) that are associated with this Protocol Group.

2.2 Spanning Tree Protocol (STP) Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

NOTE: STP is disabled by default. When you enable STP on the switch, STP is still disabled on each port.

NOTE: If STP is disabled, the system does not forward BPDU messages.

2.2.1 spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default disabled

Format `spanning-tree`

Mode Global Config

2.2.1.1 no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format `no spanning-tree`

Mode Global Config

2.2.2 spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the <slot/port> parameter to transmit a BPDU from a specified interface, or use the `all` keyword to transmit BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a "no" version.

Format `spanning-tree bpdumigrationcheck` *{*<slot/port> | *all}*

Mode Global Config

2.2.3 spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The `<name>` is a string of up to 32 characters.

Default base MAC address in hexadecimal notation

Format `spanning-tree configuration name` `<name>`

Mode Global Config

2.2.3.1 no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format `no spanning-tree configuration name`

Mode Global Config

2.2.4 spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default 0

Format `spanning-tree configuration revision` `<0-65535>`

Mode Global Config

2.2.4.1 no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format `no spanning-tree configuration revision`

Mode Global Config

2.2.5 spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format `spanning-tree edgeport`

Mode Interface Config

2.2.5.1 no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format `no spanning-tree edgeport`

Mode Interface Config

2.2.6 spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value. Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported). Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported). Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).

Default 802.1s

Format `spanning-tree forceversion` *<802.1d | 802.1s | 802.1w>*

Mode Global Config

2.2.6.1 no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value.

Format `no spanning-tree forceversion`

Mode Global Config

2.2.7 spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

Default 15

Format `spanning-tree forward-time` *<4-30>*

Mode Global Config

2.2.7.1 no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree forward-time`

Mode Global Config

2.2.8 spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree. The hello time *<value>* is in whole seconds within a range of 1 to 10, with the value being less than or equal to *(Bridge Max Age / 2) - 1*.

Default 2

Format **spanning-tree hello-time** *<1-10>*

Mode Interface Config

2.2.8.1 no spanning-tree hello-time

This command sets the admin Hello Time parameter for the common and internal spanning tree to the default value.

Format **no spanning-tree hello-time**

Mode Interface Config

2.2.9 spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to *2 x (Bridge Forward Delay - 1)*.

Default 20

Format **spanning-tree max-age** *<6-40>*

Mode Global Config

2.2.9.1 no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format **no spanning-tree max-age**

Mode Global Config

2.2.10 spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

Default 20

Format **spanning-tree max-hops** *<1-127>*

Mode Global Config

2.2.10.1 no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree max-hops`

Mode Global Config

2.2.11 spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **external-cost** option, this command sets the external-path cost for MST instance '0' i.e. CIST instance. You can set the external cost as a number in the range of 1 to 200000000 or **auto**. If you specify auto, the external path cost value is set based on Link Speed.

If you specify the **port-priority** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default cost—auto
external-cost—auto
port-priority—128

Format **`spanning-tree mst`** *<mstid> {{cost <1-200000000> | auto} | {external-cost <1-200000000> | auto} | port-priority <0-240>}*

Mode Interface Config

2.2.11.1 no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an *<mstid>* parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *<mstid>*, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **external-cost**, this command sets the external path cost for this port for mst '0' instance, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *<mstid>* parameter, to the default value.

Format **no spanning-tree mst** *<mstid> <cost | external-cost | port-priority>*

Mode Interface Config

2.2.12 spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter *<mstid>* is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default none

Format **spanning-tree mst instance** *<mstid>*

Mode Global Config

2.2.12.1 no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format **no spanning-tree mst instance** *<mstid>*

Mode Global Config

2.2.13 spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default 32768

Format **spanning-tree mst priority** *<mstid> <0-61440>*

Mode Global Config

2.2.13.1 no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter *<mstid>* is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the <mstid>, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format `spanning-tree mst priority` <*mstid*>

Mode Global Config

2.2.14 spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN so that the VLAN is no longer associated with the common and internal spanning tree. The parameter <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID.

Format `spanning-tree mst vlan` <*mstid*> <*vlanid*>

Mode Global Config

2.2.14.1 no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and a VLAN so that the VLAN is again be associated with the common and internal spanning tree. The parameter <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID.

Format `no spanning-tree mst vlan` <*mstid*> <*vlanid*>

Mode Global Config

2.2.15 spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default disabled

Format `spanning-tree port mode`

Mode Interface Config

2.2.15.1 no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format `no spanning-tree port mode`

Mode Interface Config

2.2.16 spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default disabled

Format `spanning-tree port mode all`

Mode Global Config

2.2.16.1 no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format `no spanning-tree port mode all`

Mode Global Config

2.2.17 show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format `show spanning-tree`

Modes Privileged EXEC
User EXEC

Bridge Priority Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.

Bridge Identifier The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.

Time Since Topology Change Time in seconds.

Topology Change Count Number of times changed.

Topology Change Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.

Designated Root The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.

Root Path Cost Value of the Root Path Cost parameter for the common and internal spanning tree.

Root Port Identifier Identifier of the port to access the Designated Root for the CST.

Root Port Max Age Derived value.

Root Port Bridge Forward Delay Derived value.

Hello Time Configured value of the parameter for the CST.

Bridge Hold Time Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

Bridge Max Hops Bridge max-hops count for the device.

CST Regional Root Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.

Regional Root Path Cost Path Cost to the CST Regional Root.

Associated FIDs List of forwarding database identifiers currently associated with this instance.

Associated VLANs List of VLAN IDs currently associated with this instance.

2.2.18 show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format `show spanning-tree brief`

Modes Privileged EXEC
User EXEC

Bridge Priority Configured value.

Bridge Identifier The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.

Bridge Max Age Configured value.

Bridge Max Hops Bridge max-hops count for the device.

Bridge Hello Time Configured value.

Bridge Forward Delay Configured value.

Bridge Hold Time Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

2.2.19 show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. The following details are displayed on execution of the command.

Format `show spanning-tree interface` <slot/port>

Modes Privileged EXEC
User EXEC

Hello Time Admin hello time for this port.

Port mode Enabled or disabled.

Port Up Time Since Counters Last Cleared Time since port was reset, displayed in days, hours, minutes, and seconds.

STP BPDUs Transmitted Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received Spanning Tree Protocol Bridge Protocol Data Units received.

RST BPDUs Transmitted Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RST BPDUs Received Rapid Spanning Tree Protocol Bridge Protocol Data Units received.

MSTP BPDUs Transmitted Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

2.2.20 show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <slot/port> is the desired switch port.

Format **show spanning-tree mst port detailed** <*mstid*> <slot/port>

Mode Privileged EXEC
User EXEC

MST Instance ID The ID of the existing MST instance.

Port Identifier The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.

Port Priority The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.

Port Forwarding State Current spanning tree state of this port.

Port Role Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port

Auto-Calculate Port Path Cost Indicates whether auto calculation for port path cost is enabled.

Port Path Cost Configured value of the Internal Port Path Cost parameter.

Auto-Calculate External Port Path Cost Indicates whether auto calculation for external port path cost is enabled.

External Port Path Cost Configured value of the external Port Path Cost parameter.

Designated Root The Identifier of the designated root for this port.

Designated Port Cost Path Cost offered to the LAN by the Designated Port

Designated Bridge Bridge Identifier of the bridge with the Designated Port.

Designated Port Identifier Port on the Designated Bridge that offers the lowest cost to the LAN.

If you specify 0 (defined as the default CIST ID) as the <mstid>, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. In this case, the following are displayed.

Port Identifier The port identifier for this port within the CST.

Port Priority The priority of the port within the CST.

Port Forwarding State The forwarding state of the port within the CST.

Port Role The role of the specified interface within the CST.

Port Path Cost The configured path cost for the specified interface.

Designated Root Identifier of the designated root for this port within the CST.

Designated Port Cost Path Cost offered to the LAN by the Designated Port.

Designated Bridge The bridge containing the designated port

Designated Port Identifier Port on the Designated Bridge that offers the lowest cost to the LAN

Topology Change Acknowledgement Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.

Hello Time The hello time in use for this port.

Edge Port The configured value indicating if this port is an edge port.

Edge Port Status The derived value of the edge port status. True if operating as an edge port; false otherwise.

Point To Point MAC Status Derived value indicating if this port is part of a point to point link.

CST Regional Root The regional root identifier in use for this port.

CST Port Cost The configured path cost for this port.

2.2.21 show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *<mstid>* indicates a particular MST instance. The parameter {<slot/port> | *all*} indicates the desired switch port or all ports.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the status summary displays for one or all ports within the common and internal spanning tree.

Format **show spanning-tree mst port summary** *<mstid>* {<slot/port> | *all*}

Modes Privileged EXEC
User EXEC

MST Instance ID The MST instance associated with this port.

Interface Valid slot and port number separated by forward slashes.

Type Currently not used.

STP State The forwarding state of the port in the specified spanning tree instance

Port Role The role of the specified port within the spanning tree.

Link Status The operational status of the link. Possible values are “Up” or “Down”.

Link Trap The link trap configuration for the specified interface.

2.2.22 show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format **show spanning-tree mst summary**

Modes Privileged EXEC
User EXEC

MST Instance ID List List of multiple spanning trees IDs currently configured.

For each MSTID:

Associated FIDs List of forwarding database identifiers associated with this instance.

Associated VLANs List of VLAN IDs associated with this instance.

2.2.23 show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format `show spanning-tree summary`

Modes Privileged EXEC
User EXEC

Spanning Tree Adminmode Enabled or disabled.

Spanning Tree Version Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.

Configuration Name Identifier used to identify the configuration currently being used.

Configuration Revision Level Identifier used to identify the configuration currently being used.

Configuration Digest Key Identifier used to identify the configuration currently being used.

MST Instances List of all multiple spanning tree instances configured on the switch

2.2.24 show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The *<vlanid>* corresponds to an existing VLAN ID.

Format `show spanning-tree vlan` *<vlanid>*

Modes Privileged EXEC
User EXEC

VLAN Identifier The VLANs associated with the selected MST instance.

Associated Instance Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree.

2.3 VLAN Commands

This section describes the commands you use to configure VLAN settings.

2.3.1 vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format `vlan database`

Mode Privileged EXEC

2.3.2 network mgmt_vlan

This command configures the Management VLAN ID.

Default 1

Format `network mgmt_vlan` *<1-4069>*

Mode Privileged EXEC

2.3.2.1 no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format `no network mgmt_vlan`

Mode Privileged EXEC

2.3.3 vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4094.

Format `vlan` *<2-4094>*

Mode VLAN Config

2.3.3.1 no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 2-4094.

Format `no vlan` *<2-4094>*

Mode VLAN Config

2.3.4 vlan acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default all

Format `vlan acceptframe` *{vlanonly | all}*

Mode Interface Config

2.3.4.1 no vlan acceptframe

This command resets the frame acceptance mode for the interface to the default value.

Format `no vlan acceptframe`

Mode Interface Config

2.3.5 vlan ingressfilter

This command enables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default disabled

Format `vlan ingressfilter`

Mode Interface Config

2.3.5.1 no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format `no vlan ingressfilter`

Mode Interface Config

2.3.6 vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4094.

Format `vlan makestatic` *<2-4094>*

Mode VLAN Config

2.3.7 vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4094.

Default VLAN ID 1 - default
other VLANS - blank string

Format `vlan name` *<2-4094> <name>*

Mode VLAN Config

2.3.7.1 no vlan name

This command sets the name of a VLAN to a blank string.

Format `no vlan name` *<2-4094>*

Mode VLAN Config

2.3.8 vlan participation

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format `vlan participation` *{exclude | include | auto} <1-4094>*

Mode Interface Config

Participation options are:

include The interface is always a member of this VLAN. This is equivalent to registration fixed.

exclude The interface is never a member of this VLAN. This is equivalent to registration forbidden.

auto The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

2.3.9 vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number. You can use the following participation options:

- include—The interface is always a member of this VLAN. This is equivalent to registration fixed.
- exclude—The interface is never a member of this VLAN. This is equivalent to registration forbidden.
- auto—The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

Format `vlan participation all` *{exclude | include | auto} <1-4094>*

Mode Global Config

2.3.10 vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces. The modes defined as follows:

- VLAN Only mode - Untagged frames or priority frames received on this interface are discarded.
- Admit All mode - Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default all

Format `vlan port acceptframe all` *{vlanonly | all}*

Mode Global Config

2.3.10.1 no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format `no vlan port acceptframe all`

Mode Global Config

2.3.11 vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default disabled

Format `vlan port ingressfilter all`

Mode Global Config

2.3.11.1 no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format `no vlan port ingressfilter all`

Mode Global Config

2.3.12 vlan port pvid all

This command changes the VLAN ID for all interface.

Default 1

Format `vlan port pvid all` *<1-4094>*

Mode Global Config

2.3.12.1 no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format `no vlan port pvid` *all*

Mode Global Config

2.3.13 vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `vlan port tagging all` *<1-4094>*

Mode Global Config

2.3.13.1 no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan port tagging all`

Mode Global Config

2.3.14 vlan protocol group

This command adds protocol-based VLAN groups to the system. The <*groupName*> is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

Format `vlan protocol group` <*groupname*>

Mode Global Config

2.3.15 vlan protocol group add protocol

This command adds the <*protocol*> to the protocol-based VLAN identified by <*groupid*>. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for protocol are *ip*, *arp*, and *ipx*.

NOTE: FASTPATH software supports IPv4 protocol-based VLANs.

Default none

Format `vlan protocol group add protocol` <*groupid*> <*protocol*>

Mode Global Config

2.3.15.1 no vlan protocol group add protocol

This command removes the <*protocol*> from this protocol-based VLAN group that is identified by this <*groupid*>. The possible values for protocol are *ip*, *arp*, and *ipx*.

Format `no vlan protocol group add protocol` <*groupid*> <*protocol*>

Mode Global Config

2.3.16 vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by this <*groupid*>.

Format `vlan protocol group remove` <*groupid*>

Mode Global Config

2.3.17 protocol group

This command attaches a *<vlanid>* to the protocol-based VLAN identified by *<groupid>*. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

Default none

Format **protocol group** <*groupid*> <*vlanid*>

Mode VLAN Config

2.3.17.1 no protocol group

This command removes the *<vlanid>* from this protocol-based VLAN group that is identified by this *<groupid>*.

Format **no protocol group** <*groupid*> <*vlanid*>

Mode VLAN Config

2.3.18 protocol vlan group

This command adds the physical interface to the protocol-based VLAN identified by *<groupid>*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group.

You should create the referenced VLAN before you create the protocol-based VLAN except when you configure GVRP to create the VLAN.

Default none

Format **protocol vlan group** <*groupid*>

Mode Interface Config

2.3.18.1 no protocol vlan group

This command removes the interface from this protocol-based VLAN group that is identified by this *<groupid>*.

Format **no protocol vlan group** <*groupid*>

Mode Interface Config

2.3.19 protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by *<groupid>*. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

You should create the referenced VLAN before you create the protocol-based VLAN except when you configure GVRP to create the VLAN.

Default none

Format **`protocol vlan group all`** *<groupid>*

Mode Global Config

2.3.19.1 no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this *<groupid>*.

Format **`no protocol vlan group all`** *<groupid>*

Mode Global Config

2.3.20 vlan pvid

This command changes the VLAN ID per interface.

Default 1

Format **`vlan pvid`** *<1-4094>*

Mode Interface Config

2.3.20.1 no vlan pvid

This command sets the VLAN ID per interface to 1.

Format **`no vlan pvid`**

Mode Interface Config

2.3.21 vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format **`vlan tagging`** *<1-4094>*

Mode Interface Config

2.3.21.1 no vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format **`no vlan tagging`** *<1-4094>*

Mode Interface Config

2.3.22 vlan association subnet

This command associates a VLAN to a specific IP-subnet.

Format `vlan association subnet` <*ipaddr*> <*netmask*> <*vlanid*>

Mode VLAN Config

2.3.22.1 no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format `no vlan association subnet` <*ipaddr*> <*netmask*>

Mode VLAN Config

2.3.23 vlan association mac

This command associates a MAC address to a VLAN.

Format `vlan association mac` <*macaddr*> <*vlanid*>

Mode VLAN database

2.3.23.1 no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format `no vlan association mac` <*macaddr*>

Mode VLAN database

2.3.24 show vlan

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number.

Format `show vlan` <*vlanid*>

Modes Privileged EXEC
User EXEC

VLAN ID There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4094.

VLAN Name A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of "Default." This field is optional.

VLAN Type Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).

Interface Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.

Current The degree of participation of this port in this VLAN. The permissible values are:

Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

Autodetect - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Configured The configured degree of participation of this port in this VLAN. The permissible values are:

Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

Autodetect - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Tagging The tagging behavior for this port in this VLAN.

Tagged - Transmit traffic for this VLAN as tagged frames.

Untagged - Transmit traffic for this VLAN as untagged frames.

2.3.25 show vlan brief

This command displays a list of all configured VLANs.

Format `show vlan brief`

Modes Privileged EXEC
User EXEC

VLAN ID There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4094.

VLAN Name A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.

VLAN Type Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

2.3.26 show vlan port

This command displays VLAN port information.

Format `show vlan port` *{*<slot/port> | *all}*

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.

Port VLAN ID The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.

Acceptable Frame Types The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.

Ingress Filtering May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.

GVRP May be enabled or disabled.

Default Priority The 802.1p priority assigned to tagged packets arriving on the port.

2.3.27 show vlan association subnet

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Format `show vlan association subnet` *[<ipaddr> <netmask>]*

Mode Privileged EXEC

IP Address The IP address assigned to each interface.

Net Mask The subnet mask

VLAN ID There is a VLAN Identifier (VID) associated with each VLAN.

2.3.28 show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format `show vlan association mac` *[<macaddr>]*

Mode Privileged EXEC

Mac Address A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.

VLAN ID There is a VLAN Identifier (VID) associated with each VLAN.

2.4 Double VLAN Commands

This section describes the commands you use to configure double VLAN (DVLAN). Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own 802.1Q domain.

2.4.1 dvlan-tunnel ethertype

This command configures the ether-type for all interfaces. The ether-type may have the values of *802.1Q*, *vMAN*, or *custom*. If the ether-type has a value of *custom*, the optional value of the custom ether type must be set to a value from 0 to 65535.

Default vman

Format **dvlan-tunnel ethertype** *{802.1Q | vman | custom} [0-65535]*

Mode Global Config

2.4.2 mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Default disabled

Format **mode dot1q-tunnel**

Mode Interface Config

2.4.2.1 no mode dot1q-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format **no mode dot1q-tunnel**

Mode Interface Config

2.4.3 mode dvlan-tunnel

Use this command to enable Double VLAN Tunneling on the specified interface.

NOTE: When you use the **mode dvlan-tunnel** command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

Default disabled

Format **mode dvlan-tunnel**

Mode Interface Config

2.4.3.1 no mode dvlan-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format `no mode dvlan-tunnel`

Mode Interface Config

2.4.4 show dot1q-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format `show dot1q-tunnel` *[interface {*<slot/port> | *all}]*

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

Mode The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.

EtherType A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

2.4.5 show dvlan-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format `show dvlan-tunnel` *[interface {*<slot/port> | *all}]*

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

Mode The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.

EtherType A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

2.5 Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning, which allows you to prioritize ports.

2.5.1 vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format `vlan port priority all` *<priority>*

Mode Global Config

2.5.2 vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0-7

Default 0

Format `vlan priority` *<priority>*

Mode Interface Config

2.6 Protected Ports Commands

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

2.6.1 switchport protected (Global Config)

Use this command to create a protected port group. The *<groupid>* parameter identifies the set of protected ports. Use the *name <name>* pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

NOTE: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default unprotected

Format `switchport protected` *<groupid> [name <name>]*

Mode Global Config

2.6.1.1 no switchport protected (Global Config)

Use this command to remove a protected port group. The *groupid* parameter identifies the set of protected ports. Use the **name** keyword to remove the name from the group.

Format **no switchport protected** <*groupid*> *[name]*

Mode Global Config

2.6.2 switchport protected (Interface Config)

Use this command to add an interface to a protected port group. The *<groupid>* parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

NOTE: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default unprotected

Format **switchport protected** <*groupid*>

Mode Interface Config

2.6.2.1 no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Format **no switchport protected** <*groupid*>

Mode Interface Config

2.6.3 show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format **show switchport protected** <*groupid*>

Modes Privileged EXEC
User EXEC

Group ID The number that identifies the protected port group.

Name An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

List of Physical Ports List of ports, which are configured as protected for the group identified with *<groupid>*. If no port is configured as protected for this group, this field is blank.

2.6.4 show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the groupid.

Format **show interfaces switchport** <slot/port> <*groupid*>

Mode User EXEC
Privileged EXEC

Name A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.

Protected Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group *<groupid>*

2.7 GARP Commands

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and Garp Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

2.7.1 set garp timer join

This command sets the GVRP join time for one port (Interface Config mode) or all (Global Config mode) and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default 20

Format *set garp timer join <10-100>*

Modes Interface Config
Global Config

2.7.1.1 no set garp timer join

This command sets the GVRP join time (for one or all ports and per GARP) to the default and only has an effect when GVRP is enabled.

Format *no set garp timer join*

Modes Interface Config
Global Config

2.7.2 set garp timer leave

This command sets the GVRP leave time for one port (Interface Config mode) or all ports (Global Config mode) and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds.

Default 60

Format `set garp timer leave` *<20-600>*

Modes Interface Config
Global Config

2.7.2.1 no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format `no set garp timer leave`

Modes Interface Config
Global Config

2.7.3 set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode) or a single port (Interface Config mode), and it only has an effect only when GVRP is enabled.

Default 1000

Format `set garp timer leaveall` *<200-6000>*

Modes Interface Config
Global Config

2.7.3.1 no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format `no set garp timer leaveall`

Modes Interface Config
Global Config

2.7.4 show garp

This command displays GARP information.

Format `show garp`

Modes Privileged EXEC
User EXEC

GMRP Admin Mode The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.

GVRP Admin Mode The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system

2.8 GVRP Commands

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.

NOTE: If GVRP is disabled, the system does not forward GVRP messages.

2.8.1 set gvrp adminmode

This command enables GVRP on the system.

Default disabled

Format `set gvrp adminmode`

Mode Privileged EXEC

2.8.1.1 no set gvrp adminmode

This command disables GVRP.

Format `no set gvrp adminmode`

Mode Privileged EXEC

2.8.2 set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode) or all ports (Global Config mode).

Default disabled

Format `set gvrp interfacemode`

Modes Interface Config
Global Config

2.8.2.1 no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format `no set gvrp interfacemode`

Modes Interface Config
Global Config

2.8.3 show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format `show gvrp configuration` *{*<slot/port> | *all}*

Modes Privileged EXEC
User EXEC

Interface Valid slot and port number separated by forward slashes.

Join Timer The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).

Leave Timer The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).

LeaveAll Timer This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).

Port GMRP Mode The GMRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

2.9 GMRP Commands

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP snooping, GMRP helps control the flooding of multicast packets.GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.

NOTE: If GMRP is disabled, the system does not forward GMRP messages.

2.9.1 set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default disabled

Format `set gmrp adminmode`

Mode Privileged EXEC

2.9.1.1 no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format `no set gmrp adminmode`

Mode Privileged EXEC

2.9.2 set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode) or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default disabled

Format `set gmrp interfacemode`

Modes Interface Config
Global Config

2.9.2.1 no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format `no set gmrp interfacemode`

Modes Interface Config
Global Config

2.9.3 show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format `show gmrp configuration` *{*<slot/port> | *all}*

Modes Privileged EXEC
User EXEC

Interface The slot/port of the interface that this row in the table describes.

Join Timer The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Leave Timer The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).

LeaveAll Timer This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).

Port GMRP Mode The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

2.9.4 show mac-address-table gmrp

This command displays the GMRP entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table gmrp`

Mode Privileged EXEC

Mac Address A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as 8 bytes.

Type The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description The text description of this multicast table entry.

Interfaces The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

2.10 Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (802.1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

2.10.1 authentication login

This command creates an authentication login list. The *<listname>* is any character string and is not case sensitive. Up to 10 authentication login lists can be configured on

the switch. When a list is created, the authentication method “local” is set as the first method.

When the optional parameters “Option1”, “Option2” and/or “Option3” are used, an ordered list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The maximum number of authentication login methods is three. The possible method values are **`local`**, **`radius`** and **`reject`**.

The value of **`local`** indicates that the user’s locally stored ID and password are used for authentication. The value of **`radius`** indicates that the user’s ID and password will be authenticated using the RADIUS server. The value of **`reject`** indicates the user is never authenticated.

To authenticate a user, the first authentication method in the user’s login (authentication login list) is attempted. FASTPATH software does not utilize multiple entries in the user’s login. If the first entry returns a timeout, the user authentication attempt fails.

NOTE: The default login list included with the default configuration can not be changed.

Format **`authentication login`** *<listname> [<method1> [<method2> [<method3>]]]*

Mode Global Config

2.10.1.1 no authentication login

This command deletes the specified authentication login list. The attempt to delete fails if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the non configured user for any component
- The login list is the default login list included with the default configuration and was not created using ‘authentication login’. The default login list cannot be deleted.

Format **`no authentication login`** *<listname>*

Mode Global Config

2.10.2 clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

Format **`clear dot1x statistics`** *{*<slot/port> | *all}*

Mode Privileged EXEC

2.10.3 clear radius statistics

This command is used to clear all RADIUS statistics.

Format **`clear radius statistics`**

Mode Privileged EXEC

2.10.4 dot1x defaultlogin

This command assigns the authentication login list to use for non-configured users for 802.1x port security. This setting is over-ridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format **dot1x defaultlogin** <*listname*>

Mode Global Config

2.10.5 dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format **dot1x initialize** <slot/port>

Mode Privileged EXEC

2.10.6 dot1x login

This command assigns the specified authentication login list to the specified user for 802.1x port security. The *<user>* parameter must be a configured user and the *<listname>* parameter must be a configured authentication login list.

Format **dot1x login** <*user*> <*listname*>

Mode Global Config

2.10.7 dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The *<count>* value must be in the range 1 - 10.

Default 2

Format **dot1x max-req** *<count>*

Mode Interface Config

2.10.7.1 no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format **no dot1x max-req**

Mode Interface Config

2.10.8 dot1x port-control

This command sets the authentication mode to use on the specified port. Select *force-unauthorized* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *force-authorized* to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select *auto* to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Default auto

Format **dot1x port-control** *{force-unauthorized | force-authorized | auto}*

Mode Interface Config

2.10.8.1 no dot1x port-control

This command sets the authentication mode on the specified port to the default value.

Format **no dot1x port-control**

Mode Interface Config

2.10.9 dot1x port-control all

This command sets the authentication mode to use on all ports. Select *force-unauthorized* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *force-authorized* to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select *auto* to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Default auto

Format **dot1x port-control all** *{force-unauthorized | force-authorized | auto}*

Mode Global Config

2.10.9.1 no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format **no dot1x port-control all**

Mode Global Config

2.10.10 dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format **dot1x re-authenticate** <slot/port>

Mode Privileged EXEC

2.10.11 dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Default disabled

Format `dot1x re-authentication`

Mode Interface Config

2.10.11.1 no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format `no dot1x re-authentication`

Mode Interface Config

2.10.12 dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default disabled

Format `dot1x system-auth-control`

Mode Global Config

2.10.12.1 no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format `no dot1x system-auth-control`

Mode Global Config

2.10.13 dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported.

reauth-period - The value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

quiet-period - The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.

tx-period - The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.

supp-timeout - The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.

server-timeout - The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default reauth-period: 3600 seconds
quiet-period: 60 seconds
tx-period: 30 seconds
supp-timeout: 30 seconds
server-timeout: 30 seconds

Format **`dot1x timeout`** *{{reauth-period <seconds>} | {quiet-period <seconds>} | {tx-period <seconds>} | {supp-timeout <seconds>} | {server-timeout <seconds>}}*

Mode Interface Config

2.10.13.1 no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format **`no dot1x timeout`** *{reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}*

Mode Interface Config

2.10.14 dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The `<user>` parameter must be a configured user.

Format **`dot1x user`** *<user> {*<slot/port> | *all}*

Mode Global Config

2.10.14.1 no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format **`no dot1x user`** *<user> {*<slot/port> | *all}*

Mode Global Config

2.10.15 users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format **`users defaultlogin`** *<listname>*

Mode Global Config

2.10.16 users login

This command assigns the specified authentication login list to the specified user for system login. The *<user>* must be a configured *<user>* and the *<listname>* must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete.

Note that the login list associated with the 'admin' user can not be changed to prevent accidental lockout from the switch.

Format **users login** *<user> <listname>*

Mode Global Config

2.10.17 show authentication

This command displays the ordered authentication methods for all authentication login lists.

Format **show authentication**

Mode Privileged EXEC

Authentication Login List The authentication login listname.

Method 1 The first method in the specified authentication login list, if any.

Method 2 The second method in the specified authentication login list, if any.

Method 3 The third method in the specified authentication login list, if any.

2.10.18 show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user "default" will appear in the user column.

Format **show authentication users** *<listname>*

Mode Privileged EXEC

User The user assigned to the specified authentication login list.

Component The component (User or 802.1x) for which the authentication login list is assigned.

2.10.19 show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format **show dot1x** *[{summary {*<slot/port> | *all}* | *detail* <slot/port> | *statistics* <slot/port>*]*

Mode Privileged EXEC

If you do not use any of the optional parameters, the global dot1x configuration summary is displayed.

Administrative mode Indicates whether authentication control on the switch is enabled or disabled.

If you use the optional parameter *summary {*<slot/port> | *all}*, the dot1x configuration for the specified port or all ports are displayed.

Port The interface whose configuration is displayed.

Control Mode The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto.

Operating Control Mode The control mode under which this port is operating. Possible values are authorized | unauthorized.

Reauthentication Enabled Indicates whether re-authentication is enabled on this port.

Key Transmission Enabled Indicates if the key is transmitted to the supplicant for the specified port.

If the optional parameter 'detail <slot/port>' is used, the detailed dot1x configuration for the specified port are displayed.

Port The interface whose configuration is displayed.

Protocol Version The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.

PAE Capabilities The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.

Authenticator PAE State Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.

Backend Authentication State Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.

Quiet Period The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.

Transmit Period The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.

Supplicant Timeout The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.

Server Timeout The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.

Maximum Requests The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.

Reauthentication Period The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.

Reauthentication Enabled Indicates if reauthentication is enabled on this port. Possible values are ‘True” or “False”.

Key Transmission Enabled Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.

Control Direction The control direction for the specified port or ports. Possible values are both or in.

If you use the optional parameter **`statistics`** <slot/port>, the following dot1x statistics for the specified port appear.

Port The interface whose statistics are displayed.

EAPOL Frames Received The number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted The number of EAPOL frames of any type that have been transmitted by this authenticator.

EAPOL Start Frames Received The number of EAPOL start frames that have been received by this authenticator.

EAPOL Logoff Frames Received The number of EAPOL logoff frames that have been received by this authenticator.

Last EAPOL Frame Version The protocol version number carried in the most recently received EAPOL frame.

Last EAPOL Frame Source The source MAC address carried in the most recently received EAPOL frame.

EAP Response/Id Frames Received The number of EAP response/identity frames that have been received by this authenticator.

EAP Response Frames Received The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.

EAP Request/Id Frames Transmitted The number of EAP request/identity frames that have been transmitted by this authenticator.

EAP Request Frames Transmitted The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.

Invalid EAPOL Frames Received The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

EAP Length Error Frames Received The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

2.10.20 show dot1x users

This command displays 802.1x port security user information for locally configured users.

Format `show dot1x users` <slot/port>

Mode Privileged EXEC

User Users configured locally to have access to the specified port.

2.10.21 show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

Format `show users authentication`

Mode Privileged EXEC

User Lists every user that has an authentication login list assigned.

System Login The authentication login list assigned to the user for system login.

802.1x Port Security The authentication login list assigned to the user for 802.1x port security.

2.11 Storm-Control Commands

This section describes commands you use to configure storm control and view storm-control configuration information. The Storm Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis. The Storm Control feature can help maintain network performance.

2.11.1 storm-control broadcast

Use this command to enable broadcast storm recovery mode for a specific interface. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control broadcast`

Mode Interface Config

2.11.1.1 no storm-control broadcast

Use this command to disable broadcast storm recovery mode for a specific interface.

Format `no storm-control broadcast`

Mode Interface Config

2.11.2 storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for an interface. When you use this command, broadcast storm recovery mode is enabled on the interface and broadcast storm recovery is active. If the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 5

Format **`storm-control broadcast level`** *`<0-100>`*

Mode Interface Config

2.11.2.1 no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format **`no storm-control broadcast level`**

Mode Interface Config

2.11.3 storm-control broadcast all

This command enables broadcast storm recovery mode for all interfaces. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default disabled

Format **`storm-control broadcast all`**

Mode Global Config

2.11.3.1 no storm-control broadcast all

This command disables broadcast storm recovery mode for all interfaces.

Format **`no storm-control broadcast all`**

Mode Global Config

2.11.4 storm-control broadcast all level

This command configures the broadcast storm recovery threshold for all interfaces. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.This command also enables broadcast storm recovery mode for all interfaces.

Default 5

Format **`storm-control broadcast all level`** <0-100>

Mode Global Config

2.11.4.1 no storm-control broadcast all level

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format `no storm-control broadcast all level`

Mode Global Config

2.11.5 storm-control multicast

This command enables multicast storm recovery mode for an interface. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control multicast`

Mode Interface Config

2.11.5.1 no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Format `no storm-control multicast`

Mode Interface Config

2.11.6 storm-control multicast level

This command configures the multicast storm recovery threshold for an interface and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control multicast level` <0-100>

Mode Interface Config

2.11.6.1 no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format `no storm-control multicast level`

Mode Interface Config

2.11.7 storm-control multicast all

This command enables multicast storm recovery mode for all interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be

dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control multicast all`

Mode Global Config

2.11.7.1 no storm-control multicast all

This command disables multicast storm recovery mode for all interfaces.

Format `no storm-control multicast all`

Mode Global Config

2.11.8 storm-control multicast all level

This command configures the multicast storm recovery threshold for all interfaces and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control multicast all level` <0-100>

Mode Global Config

2.11.8.1 no storm-control multicast all level

This command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

Format `no storm-control multicast all level`

Mode Global Config

2.11.9 storm-control unicast

This command enables unicast storm recovery mode for an interface. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control unicast`

Mode Interface Config

2.11.9.1 no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Format `no storm-control unicast`

Mode Interface Config

2.11.10 storm-control unicast level

This command configures the unicast storm recovery threshold for an interface and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default 5

Format `storm-control unicast level` <0-100>

Mode Interface Config

2.11.10.1 no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Format `no storm-control unicast level`

Mode Interface Config

2.11.11 storm-control unicast all

This command enables unicast storm recovery mode for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control unicast all`

Mode Global Config

2.11.11.1 no storm-control unicast all

This command disables unicast storm recovery mode for all interfaces.

Format `no storm-control unicast all`

Mode Global Config

2.11.12 storm-control unicast all level

This command configures the unicast storm recovery threshold and enables unicast storm recovery for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control unicast all level` <0-100>

Mode Global Config

2.11.12.1 no storm-control unicast all level

This command returns the unicast storm recovery threshold to the default value and disables unicast storm recovery for all interfaces.

Format `no storm-control unicast all level`

Mode Global Config

2.11.13 storm-control flowcontrol

This command enables 802.3x flow control for the switch and only applies to full-duplex mode ports.

NOTE: 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

Default disabled

Format `storm-control flowcontrol`

Mode Global Config

2.11.13.1 no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

NOTE: This command only applies to full-duplex mode ports.

Format `no storm-control flowcontrol`

Mode Global Config

2.11.14 show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters. Use the `all` keyword to display the per-port configuration parameters for all interfaces, or specify the slot/port to display information about a specific interface.

Format `show storm-control` *[all* | <slot/port>*]*

Mode Privileged EXEC

Bcast Mode Shows whether the broadcast storm control mode is enabled or disabled.

Bcast Level The broadcast storm control level.

Mcast Mode Shows whether the multicast storm control mode is enabled or disabled.

Mcast Level The multicast storm control level.

Ucast Mode Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.

Ucast Level The Unknown Unicast or DLF (Destination Lookup Failure) storm control level

2.12 Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address.Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.

NOTE: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

2.12.1 port-channel

This command configures a new port-channel (LAG) and generates a logical slot/port number for the port-channel. The *<name>* field is a character string which allows the dash "-" character as well as alphanumeric characters. Use the **`show port channel`** command to display the slot/port number for the logical interface.

NOTE: Before you include a port in a port-channel, set the port physical mode. For more information, see 2.1.8 "speed" on page 2 - 4.

Format **`port-channel`** *<name>*

Mode Global Config

2.12.1.1 no port-channel

This command deletes a port-channel (LAG).

Format **`no port-channel`** *{<logical* slot/port> | *all}*

Mode Global Config

2.12.2 addport

This command adds one port to the port-channel (LAG). The first interface is a logical slot/port number of a configured port-channel.

NOTE: Before adding a port to a port-channel, set the physical mode of the port. For more information, see 2.1.8 “speed” on page 2 - 4.

Format `addport` <*logical* slot/port>

Mode Interface Config

2.12.3 deleteport (Interface Config)

This command deletes the port from the port-channel (LAG). The interface is a logical slot/port number. of a configured port-channel.

Format `deleteport` <*logical* slot/port>

Mode Interface Config

2.12.4 deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical slot/port number. of a configured port-channel. To clear the port channels, see 4.5.6 “clear port-channel” on page 4 - 25

Format `deleteport` *{*<*logical* slot/port> | *all}*

Mode Global Config

2.12.5 port-channel static

This command enables the static mode on a port-channel (LAG) interface. By default the static mode for a new port-channel is disabled, which means the port-channel is dynamic. However if the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel enabled, which means the port-channel is static.You can only use this command on port-channel interfaces.

Default disabled

Format `port-channel static`

Mode Interface Config

2.12.5.1 no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format `no port-channel static`

Mode Interface Config

2.12.6 port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port.

Default enabled

Format `port lacpmode`

Mode Interface Config

2.12.6.1 no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format `no port lacpmode`

Mode Interface Config

2.12.7 port lacpmode all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format `port lacpmode all`

Mode Global Config

2.12.7.1 no port lacpmode all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format `no port lacpmode all`

Mode Global Config

2.12.8 port lacp timeout (Interface Config)

This command sets the timeout on a physical interface of a particular device type (**actor** or **partner**) to either **long** or **short** timeout.

Default long

Format `port lacp timeout` *{actor | partner} {long | short}*

Mode Interface Config

2.12.8.1 no port lacp timeout

This command sets the timeout back to its default value on a physical interface of a particular device type (**actor** or **partner**).

Format `no port lacp timeout` *{actor | partner}*

Mode Interface Config

2.12.9 port lacp timeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (**actor** or **partner**) to either **long** or **short** timeout.

Default long

Format `port lacp timeout` *{actor | partner} {long | short}*

Mode Global Config

2.12.9.1 no port lacp timeout

This command sets the timeout for all physical interfaces of a particular device type (**actor** or **partner**) back to their default values.

Format `no port lacp timeout` *{actor | partner}*

Mode Global Config

2.12.10 port-channel adminmode

This command enables a port-channel (LAG). The option **all** sets every configured port-channel with the same administrative mode setting.

Format **port-channel adminmode** *[all]*

Mode Global Config

2.12.10.1 no port-channel adminmode

This command disables a port-channel (LAG). The option **all** sets every configured port-channel with the same administrative mode setting.

Format **no port-channel adminmode** *[all]*

Mode Global Config

2.12.11 port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Default enabled

Format **port-channel linktrap** *{<logical* slot/port> | *all}*

Mode Global Config

2.12.11.1 no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Format **no port-channel linktrap** *{<logical* slot/port> | *all}*

Mode Global Config

2.12.12 port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical slot/port for a configured port-channel, and *<name>* is an alphanumeric string up to 15 characters.

Format **port-channel name** *{<logical* slot/port> | *all* | *<name>}*

Mode Global Config

2.12.13 show port-channel brief

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces.

Format **show port-channel brief**

Modes Privileged EXEC
User EXEC

For each port-channel the following information is displayed:

Logical Interface The slot/port of the logical interface.

Port-channel Name The name of port-channel (LAG) interface.

Link-State Shows whether the link is up or down.

Type Shows whether the port-channel is statically or dynamically maintained.

LACP Device Type/Timeout The timeout (**long** or **short**) for the type of device (**actor** or **partner**)

Mbr Ports The members of this port-channel.

Active Ports The ports that are actively participating in the port-channel.

2.12.14 show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

Format `show port-channel` *{<logical* slot/port> | *all}*

Modes Privileged EXEC
User EXEC

Logical Interface Valid slot and port number separated by forward slashes.

Port-Channel Name The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.

Link State Indicates whether the Link is up or down.

Admin Mode May be enabled or disabled. The factory default is enabled.

Mbr Ports A listing of the ports that are members of this port-channel (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).

Device Timeout For each port, lists the timeout (**long** or **short**) for Device Type (**actor** or **partner**)

Port Speed Speed of the port-channel port.

Type The status designating whether a particular port-channel (LAG) is statically or dynamically maintained.

Static - The port-channel is statically maintained.

Dynamic - The port-channel is dynamically maintained.

Active Ports This field lists ports that are actively participating in the port-channel (LAG).

2.13 Port Mirroring

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

2.13.1 monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the *source interface* <slot/port> parameter to specify the interface to monitor. Use *rx* to monitor only ingress packets, or use *tx* to monitor only egress packets. If you do not specify an *{rx | tx}* option, the destination port monitors both ingress and egress packets. Use the *destination interface* <slot/port> to specify the interface to receive the monitored traffic. Use the *mode* parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Format **monitor session** <*session-id*> *{source interface* <slot/port> *[{rx | tx}]* | *destination interface* <slot/port> | *mode}*

Mode Global Config

2.13.1.1 no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs. Use the *source interface* <slot/port> parameter or *destination interface* <slot/port> to remove the specified interface from the port monitoring session. Use the *mode* parameter to disable the administrative mode of the session.

NOTE: Since the current version of FASTPATH software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the **no monitor** command.

Format **no monitor session** <*session-id*> *[{source interface* <slot/port> | *destination interface* <slot/port> | *mode}]*

Mode Global Config

2.13.2 no monitor

This command removes all the source ports and a destination port for the and restores the default value for mirroring session mode for all the configured sessions.

NOTE: This is a stand-alone “no” command. This command does not have a “normal” form.

Default enabled

Format **no monitor**

Mode Global Config

2.13.3 show monitor session

This command displays the Port monitoring information for a particular mirroring session.

NOTE: The <session-id> parameter is an integer value used to identify the session. In the current version of the software, the <session-id> parameter is always one (1).

Format **show monitor session** <session-id>

Mode Privileged EXEC

Session ID An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.

Monitor Session Mode Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <session-id>. The possible values are Enabled and Disabled.

Probe Port Probe port (destination port) for the session identified with <session-id>. If probe port is not set then this field is blank.

Source Port The port, which is configured as mirrored port (source port) for the session identified with <session-id>. If no source port is configured for the session then this field is blank.

Type Direction in which source port configured for port mirroring.Types are tx for transmitted packets and rx for receiving packets.

2.14 Static MAC Filtering

The commands in this section describe how to configure static MAC filtering.

2.14.1 macfilter

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The value of the <macaddr> parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The <vlanid> parameter must identify a valid VLAN. You can create up to 100 static MAC filters.

Format **macfilter** <*macaddr*> <*vlanid*>

Mode Global Config

2.14.1.1 no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN.

Format **no macfilter** <*macaddr*> <*vlanid*>

Mode Global Config

2.14.2 macfilter addsrc

This command adds the interface to the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format **macfilter addsrc** *<macaddr> <vlanid>*

Mode Interface Config

2.14.2.1 no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of *<macaddr>* and VLAN of *<vlanid>*. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format **no macfilter addsrc** *<macaddr> <vlanid>*

Mode Interface Config

2.14.3 macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of *<macaddr>* and *<vlanid>*. You must specify the *<macaddr>* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format **macfilter addsrc all** *<macaddr> <vlanid>*

Mode Global Config

2.14.3.1 no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of *<macaddr>* and VLAN of *<vlanid>*. You must specify the *<macaddr>* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *<vlanid>* parameter must identify a valid VLAN.

Format **no macfilter addsrc all** *<macaddr> <vlanid>*

Mode Global Config

2.14.4 show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you select *<all>*, all the Static MAC Filters in the system are displayed. If you supply a value for *<macaddr>*, you must also enter a value for *<vlanid>*, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Format **show mac-address-table static** *{<macaddr> <vlanid> | all}*

Mode Privileged EXEC

MAC Address The MAC Address of the static MAC filter entry.

VLAN ID The VLAN ID of the static MAC filter entry.

Source Port(s) The source port filter set's slot and port(s).

2.14.5 show mac-address-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table staticfiltering`

Mode Privileged EXEC

Mac Address A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.

Type The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description The text description of this multicast table entry.

Interfaces The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

2.15 IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. FASTPATH software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

2.15.1 set igmp

This command enables IGMP Snooping on the system (Global Config Mode) or an interface (Interface Config Mode). This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default disabled

Format `set igmp`

Modes Global Config
Interface Config

Format `set igmp <vlanid>`

Mode VLAN Config

2.15.1.1 no set igmp

This command disables IGMP Snooping on the system, an interface or a VLAN.

Format `no set igmp`

Modes Global Config
Interface Config

Format `no set igmp <vlanid>`

Mode VLAN Config

2.15.2 set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default disabled

Format `set igmp interfacemode`

Mode Global Config

2.15.2.1 no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format `no set igmp interfacemode`

Mode Global Config

2.15.3 set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default disabled

Format `set igmp fast-leave`

Mode Interface Config

Format `set igmp fast-leave` *<vlan_id>*

Mode VLAN Config

2.15.3.1 no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format `no set igmp fast-leave`

Modes Interface Config

Format `no set igmp fast-leave` *<vlan_id>*

Mode VLAN Config

2.15.4 set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default 260 seconds

Format `set igmp groupmembership-interval` *<2-3600>*

Modes Interface Config
Global Config

Format `set igmp groupmembership-interval` *<vlan_id> <2-3600>*

Modes VLAN Config

2.15.4.1 no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format `no set igmp groupmembership-interval`

Modes Interface Config
Global Config

Format `no set igmp groupmembership-interval` *<vlan_id>*

Mode VLAN Config

2.15.5 set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, or on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3599 seconds.

Default 10 seconds

Format **set igmp maxresponse** *<1-3599>*

Modes Global Config
Interface Config

Format **set igmp maxresponse** *<vlan_id> <1-3599>*

Mode VLAN Config

2.15.5.1 no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format **no set igmp maxresponse**

Modes Global Config
Interface Config

Format **no set igmp maxresponse** *<vlan_id>*

Mode VLAN Config

2.15.6 set igmp mcrtexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

Default 0

Format **set igmp mcrtexpiretime** *<0-3600>*

Modes Global Config
Interface Config

Format **set igmp mcrtexpiretime** *<vlan_id> <0-3600>*

Mode VLAN Config

2.15.6.1 no set igmp mcrtexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format **no set igmp mcrtexpiretime**

Modes Global Config
Interface Config

Format **no set igmp mcrtexpiretime** *<vlan_id>*

Mode VLAN Config

2.15.7 set igmp mrouter

This command configures the VLAN ID (<vlan_id>) that has the multicast router mode enabled.

Format `set igmp mrouter <vlan_id>`

Mode Interface Config

2.15.7.1 no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (<vlan_id>) .

Format `no set igmp mrouter <vlan_id>`

Mode Interface Config

2.15.8 set igmp mrouter interface

This command configures the interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default disabled

Format `set igmp mrouter interface`

Mode Interface Config

2.15.8.1 no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format `no set igmp mrouter interface`

Mode Interface Config

2.15.9 show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

Format `show igmpsnooping` *[*<slot/port> | *<vlan_id>]*

Mode Privileged EXEC

When the optional arguments <slot/port> or <vlan_id> are not used, the command displays the following information:

Admin Mode Indicates whether or not IGMP Snooping is active on the switch.

Multicast Control Frame Count The number of multicast control frames that are processed by the CPU.

Interface Enabled for IGMP Snooping The list of interfaces on which IGMP Snooping is enabled.

VLANS Enabled for IGMP Snooping A list of VLANS on which IGMP Snooping is enabled.

When you specify the <slot/port> values, the following information appears:

IGMP Snooping Admin Mode Indicates whether IGMP Snooping is active on the interface.

Fast Leave Mode Indicates whether IGMP Snooping Fast-leave is active on the interface.

Group Membership Interval The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.This value may be configured

Maximum Response Time The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.

Multicast Router Expiry Time The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *<vlan_id>*, the following information appears:

VLAN ID The VLAN ID.

IGMP Snooping Admin Mode Indicates whether IGMP Snooping is active on the VLAN.

Fast Leave Mode ndicates whether IGMP Snooping Fast-leave is active on the VLAN.

Group Membership Interval The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry.This value may be configured.

Maximum Response Time The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.

Multicast Router Expiry Time The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

2.15.10 show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter interface` <slot/port>

Mode Privileged EXEC

Interface The port on which multicast router information is being displayed.

Multicast Router Attached Indicates whether multicast router is statically enabled on the interface.

VLAN ID The list of VLANs of which the interface is a member.

2.15.11 show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter vlan` <slot/port>

Mode Privileged EXEC

Interface The port on which multicast router information is being displayed.

VLAN ID The list of VLANs of which the interface is a member.

2.15.12 show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format `show mac-address-table igmpsnooping`

Mode Privileged EXEC

MAC Address A multicast MAC address for which the switch has forwarding or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as a MAC address and VLAN ID combination of 8 bytes.

Type The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).

Description The text description of this multicast table entry.

Interfaces The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

2.16 Port Security Commands

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

NOTE: To enable the SNMP trap specific to port security, see 5.6.8 “snmp-server enable traps violation” on page 5 - 18.

2.16.1 port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config)

Default disabled

Format `port-security`

Modes Global Config
Interface Config

2.16.1.1 no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format `no port-security`

Modes Global Config
Interface Config

2.16.2 port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Default 600

Format **port-security max-dynamic** *<maxvalue>*

Mode Interface Config

2.16.2.1 no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format **no port-security max-dynamic**

Mode Interface Config

2.16.3 port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port.

Default 20

Format **port-security max-static** *<maxvalue>*

Mode Interface Config

2.16.3.1 no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format **no port-security max-static**

Mode Interface Config

2.16.4 port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses. The *<vid>* is the VLAN ID.

Format **port-security mac-address** *<mac-address> <vid>*

Mode Interface Config

2.16.4.1 no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format **no port-security mac-address** *<mac-address> <vid>*

Mode Interface Config

2.16.5 port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses.

Format `port-security mac-address move`

Mode Interface Config

2.16.6 show port-security

This command displays the port-security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

Format `show port-security` *[{*<slot/port> | *all}]*

Mode Privileged EXEC

Admin Mode Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information appears:

Admin Mode Port Locking mode for the Interface.

Dynamic Limit Maximum dynamically allocated MAC Addresses.

Static Limit Maximum statically allocated MAC Addresses.

Violation Trap Mode Whether violation traps are enabled.

2.16.7 show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

Format `show port-security dynamic` <slot/port>

Mode Privileged EXEC

MAC Address MAC Address of dynamically locked MAC.

2.16.8 show port-security static

This command displays the statically locked MAC addresses for port.

Format `show port-security static` <slot/port>

Mode Privileged EXEC

MAC Addres MAC Address of statically locked MAC.

2.16.9 show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Format `show port-security violation` <slot/port>

Mode Privileged EXEC

MAC Address MAC Address of discarded packet on locked port.

2.17 LLDP (802.1AB) Commands

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

2.17.1 lldp transmit

Use this command to enable the LLDP advertise capability.

Default disabled

Format `lldp transmit`

Mode Interface Config

2.17.1.1 no lldp transmit

Use this command to return the local data transmission capability to the default.

Format `no lldp transmit`

Mode Interface Config

2.17.2 lldp receive

Use this command to enable the LLDP receive capability.

Default disabled

Format `lldp receive`

Mode Interface Configuration

2.17.2.1 no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format `lldp receive`

Mode Interface Configuration

2.17.3 lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *<interval-seconds>* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The *<hold-value>* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The *<reinit-seconds>* is the delay before re-initialization, and the range is 1-0 seconds.

Default interval—30 seconds
hold—4
reinit—2 seconds

Format *lldp timers [interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>*]

Mode Global Config

2.17.3.1 no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format **`no lldp timers`** *[interval] [hold] [reinit]*

Mode Global Config

2.17.4 lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use *`sys-name`* to transmit the system name TLV. To configure the system name, see 5.6.1 “snmp-server“on page 5 - 15. Use *`sys-desc`*to transmit the system description TLV. Use *`sys-cap`* to transmit the system capabilities TLV. Use *`port-desc`* to transmit the port description TLV. To configure the port description, see 2.1.4 “description“on page 2 - 3.

Default no optional TLVs are included

Format **`lldp transmit-tlv`** *[sys-desc] [sys-name] [sys-cap] [port-desc]*

Mode Interface Config

2.17.4.1 no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format **`no lldp transmit-tlv`** *[sys-desc] [sys-name] [sys-cap] [port-desc]*

Mode Interface Config

2.17.5 lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs.

Format **`lldp transmit-mgmt`**

Mode Interface Config

2.17.5.1 no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format **`no lldp transmit-mgmt`**

Mode Interface Config

2.17.6 lldp notification

Use this command to enable remote data change notifications.

Default disabled

Format `lldp notification`

Mode Interface Config

2.17.6.1 no lldp notification

Use this command to disable notifications.

Default disabled

Format `no lldp notification`

Mode Interface Config

2.17.7 lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The *<interval>* parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default 5

Format `lldp notification-interval` *<interval>*

Mode Global Config

2.17.7.1 no lldp notification-interval

Use this command to return the notification interval to the default value.

Format `no lldp notification-interval`

Mode Global Config

2.17.8 clear lldp statistics

Use this command to reset all LLDP statistics.

Format `clear lldp statistics`

Mode Global Config

2.17.9 clear lldp remote-data

Use this command to delete all information from the LLDP remote data table.

Format `clear lldp remote-data`

Mode Global Config

2.17.10 show lldp

Use this command to display a summary of the current LLDP configuration.

Format `show lldp`

Mode Privileged EXEC

Transmit Interval How frequently the system transmits local data LLDPDUs, in seconds.

Transmit Hold Multiplier The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.

Re-initialization Delay The delay before re-initialization, in seconds.

Notification Interval How frequently the system sends remote data change notifications, in seconds.

2.17.11 show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format `show lldp interface` *{*<slot/port> | *all}*

Mode Privileged EXEC.

Interface The interface in a slot/port format.

Link Shows whether the link is up or down.

Transmit Shows whether the interface transmits LLDPDUs.

Receive Shows whether the interface receives LLDPDUs.

Notify Shows whether the interface sends remote data change notifications.

TLVs Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).

Mgmt Shows whether the interface transmits system management address information in the LLDPDUs.

2.17.12 show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format `show lldp statistics` *{*<slot/port> | *all}*

Mode Privileged EXEC

Last Update The amount of time since the last update to the remote table in days, hours, minutes, and seconds.

Total Inserts Total number of inserts to the remote data table.

Total Deletes Total number of deletes from the remote data table.

Total Drops Total number of times the complete remote data received was not inserted due to insufficient resources.

Total Ageouts Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Interface The interface in slot/port format.

Transmit Total Total number of LLDP packets transmitted on the port.

Receive Total Total number of LLDP packets received on the port.

Discards Total number of LLDP frames discarded on the port for any reason.

Errors The number of invalid LLDP frames received on the port.

Ageouts Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.

TVL Discards The number of TLVs discarded

TVL Unknowns Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

2.17.13 show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format `show lldp remote-device` *{*<slot/port> | *all}*

Mode Privileged EXEC

Local Interface The interface that received the LLDPDU from the remote device.

Chassis ID The ID of the remote device.

Port ID The port number that transmitted the LLDPDU.

System Name The system name of the remote device.

2.17.14 show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format `show lldp remote-device detail` <slot/port>

Mode Privileged EXEC

Local Interface The interface that received the LLDPDU from the remote device.

Chassis ID Subtype The type of identification used in the Chassis ID field.

Chassis ID The chassis of the remote device.

Port ID Subtype The type of port on the remote device.

Port ID The port number that transmitted the LLDPDU.

System Name The system name of the remote device.

System Description Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.

Port Description Describes the port in an alpha-numeric format. The port description is configurable.

System Capabilities Supported Indicates the primary function(s) of the device.

System Capabilities Enabled Shows which of the supported system capabilities are enabled.

Management Address For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.

Time To Live The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

2.17.15 show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format `show lldp local-device` *{*<slot/port> | *all}*

Mode Privileged EXEC

Interface The interface in a slot/port format.

Port ID The port ID associated with this interface.

Port Description The port description associated with the interface.

2.17.16 show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format `show lldp local-device detail` <slot/port>

Mode Privileged EXEC

Interface The interface that sends the LLDPDU.

Chassis ID Subtype The type of identification used in the Chassis ID field.

Chassis ID The chassis of the local device.

Port ID Subtype The type of port on the local device.

Port ID The port number that transmitted the LLDPDU.

System Name The system name of the local device.

System Description Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.

Port Description Describes the port in an alpha-numeric format.

System Capabilities Supported Indicates the primary function(s) of the device.

System Capabilities Enabled Shows which of the supported system capabilities are enabled.

Management Address The type of address and the specific address the local LLDP agent uses to send and receive information.

2.18 Denial of Service Commands

This section describes the commands you use to configure DoS Control. FASTPATH software provides support for classifying and blocking specific types of Denial of

Service attacks. You can configure your system to monitor and block six types of attacks:

- **SIP=DIP:** Source IP address = Destination IP address.
- **First Fragment:** TCP Header size smaller then configured value.
- **TCP Fragment:** IP Fragment Offset = 1.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.

2.18.1 dos-control sipdip

This command enables Source IP address = Destination IP address (SIP=DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP=DIP, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control sipdip`

Mode Global Config

2.18.1.1 no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP=DIP) Denial of Service prevention.

Format `no dos-control sipdip`

Mode Global Config

2.18.2 dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled.The default is *disabled*. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to *20*.

Default disabled <20>

Format `dos-control firstfrag` [<0-255>]

Mode Global Config

2.18.2.1 no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of *disabled*.

Format `no dos-control firstfrag`

Mode Global Config

2.18.3 dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control tcpfrag`

Mode Global Config

2.18.3.1 no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

Format `no storm-control broadcast all`

Mode Global Config

2.18.4 dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control tcpflag`

Mode Global Config

2.18.4.1 no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format `no dos-control tcpflag`

Mode Global Config

2.18.5 dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

NOTE: Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Default disabled

Format `dos-control l4port`

Mode Global Config

2.18.5.1 no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format `no dos-control l4port`

Mode Global Config

2.18.6 dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default disabled <512>

Format `dos-control icmp` *<0-1023>*

Mode Global Config

2.18.6.1 no dos-control icmp

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format `no dos-control icmp`

Mode Global Config

2.18.7 show dos-control

This command displays Denial of Service configuration information.

Format `show dos-control`

Mod Privileged EXEC

SIPDIP Mode May be enabled or disabled. The factory default is disabled.

First Fragment Mode May be enabled or disabled. The factory default is disabled.

Min TCP Hdr Size <0-255> The factory default is 20.

TCP Fragment Mode May be enabled or disabled. The factory default is disabled.

TCP Flag Mode May be enabled or disabled. The factory default is disabled.

L4 Port Mode May be enabled or disabled. The factory default is disabled.

ICMP Mode May be enabled or disabled. The factory default is disabled.

Max ICMP Pkt Size <0-1023> The factory default is 512.

2.19 MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

2.19.1 bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The *<seconds>* parameter must be within the range of 10 to 1,000,000 seconds.

Default 300

Format **bridge aging-time** *<10-1,000,000>*

Mode Global Config

2.19.1.1 no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Format **no bridge aging-time**

Mode Global Config

2.19.2 show forwardingdb agetime

This command displays the timeout for address aging. In an IVL system, the [fdbid | all] parameter is required.

Default all

Format **show forwardingdb agetime** *[fdbid | all]*

Mode Privileged EXEC

Forwarding DB ID Fdbid (Forwarding database ID) indicates the forwarding database whose aging timeout is to be shown. The all option is used to display the aging timeouts associated with all forwarding databases. This field displays the forwarding database ID in an IVL system.

Agetime In an IVL system, this parameter displays the address aging timeout for the associated forwarding database.

2.19.3 show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format **show mac-address-table multicast** *<macaddr>*

Mode Privileged EXEC

MAC Address A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as a MAC address and VLAN ID combination of 8 bytes.

Type The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Component The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.

Description The text description of this multicast table entry.

Interfaces The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Forwarding Interfaces The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

2.19.4 show mac-address-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format `show mac-address-table stats`

Mode Privileged EXEC

Total Entries The total number of entries that can possibly be in the Multicast Forwarding Database table.

Most MFDB Entries Ever Used The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.

Current Entries The current number of entries in the MFDB.



Chapter 3

Quality of Service Commands

3. Quality of Service (QoS) Commands

This chapter describes the Quality of Service (QoS) commands available in the CLI.

The QoS Commands chapter contains the following sections:

- 3.1 “Class of Service (CoS) Commands” on page 3 - 2
- 3.2 “Differentiated Services (DiffServ) Commands” on page 3 - 6
- 3.3 “DiffServ Class Commands” on page 3 - 7
- 3.4 “DiffServ Policy Commands” on page 3 - 12
- 3.5 “DiffServ Service Commands” on page 3 - 15
- 3.6 “DiffServ Show Commands” on page 3 - 16
- 3.7 “MAC Access Control List (ACL) Commands” on page 3 - 20
- 3.8 “IP Access Control List (ACL) Commands” on page 3 - 23

The commands in this chapter are in one of two functional groups:

- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display device settings, statistics and other information.

3.1 Class of Service (CoS) Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

NOTE: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

3.1.1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *<userpriority>* values can range from 0-7. The *<trafficclass>* values range from 0-6, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see 2.5 “Provisioning (IEEE 802.1p) Commands” on page 2 - 29.

Format `classofservice dot1p-mapping` *<userpriority> <trafficclass>*

Modes Global Config
Interface Config

3.1.1.1 no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format `no classofservice dot1p-mapping`

Modes Global Config
Interface Config

3.1.2 classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The *<ipdscp>* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

The *<trafficclass>* values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format **classofservice ip-dscp-mapping** *<ipdscp> <trafficclass>*

Mode Global Config

3.1.2.1 no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format **no classofservice ip-dscp-mapping**

Mode Global Config

3.1.3 classofservice trust

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the **show running config** command because Dot1p is the default.

NOTE: The **classofservice trust dot1p** command will not be supported in future releases of the software because Dot1p is the default value. Use the **no classofservice trust** command to set the mode to the default value.

Default dot1p

Format **classofservice trust** *{dot1p | ip-dscp | ip-precedence | untrusted}*

Mode Global Config
Interface Config

3.1.3.1 no classofservice trust

This command sets the interface mode to the default value.

Format **no classofservice trust**

Modes Global Config
Interface Config

3.1.4 cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The total number of queues supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format **cos-queue min-bandwidth** *<bw-0> <bw-1> ... <bw-n>*

Modes Global Config
Interface Config

3.1.4.1 no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format `no cos-queue min-bandwidth`

Modes Global Config
Interface Config

3.1.5 cos-queue strict

This command activates the strict priority scheduler mode for each specified queue.

Format `cos-queue strict` *<queue-id-1> [<queue-id-2> ... <queue-id-n>]*

Modes Global Config
Interface Config

3.1.5.1 no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format `no cos-queue strict` *<queue-id-1> [<queue-id-2> ... <queue-id-n>]*

Modes Global Config
Interface Config

3.1.6 traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format `traffic-shape` *<bw>*

Modes Global Config
Interface Config

3.1.6.1 no traffic-shape

This command restores the interface shaping rate to the default value.

Format `no traffic-shape`

Modes Global Config
Interface Config

3.1.7 show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The <slot/port> parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed. For more information, see 2.5 “Provisioning (IEEE 802.1p) Commands” on page 2 - 29.

Format `show classofservice dot1p-mapping` *[*<slot/port>*]*

Mode Privileged EXEC

The following information is repeated for each user priority.

User Priority The 802.1p user priority value.

Traffic Class The traffic class internal queue identifier to which the user priority value is mapped.

3.1.8 show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show classofservice ip-precedence-mapping` *[*<slot/port>*]*

Mode Privileged EXEC

The following information is repeated for each user priority.

IP Precedence The IP Precedence value.

Traffic Class The traffic class internal queue identifier to which the IP Precedence value is mapped.

3.1.9 show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format `show classofservice ip-dscp-mapping`

Mode Privileged EXEC

The following information is repeated for each user priority.

IP DSCP The IP DSCP value.

Traffic Class The traffic class internal queue identifier to which the IP DSCP value is mapped.

3.1.10 show classofservice trust

This command displays the current trust mode setting for a specific interface. The <slot/port> parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

Format `show classofservice trust` *[*<slot/port>*]*

Mode Privileged EXEC

Non-IP Traffic Class The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).

Untrusted Traffic Class The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

3.1.11 show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show interfaces cos-queue` *[*<slot/port>*]*

Mode Privileged EXEC

Queue Id An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.

Minimum Bandwidth The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.

Scheduler Type Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.

Queue Management Type The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Interface The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.

Interface Shaping Rate The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

3.2 Differentiated Services (DiffServ) Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
   - Creating and deleting classes.
   - Defining match criteria for a class.
2. Policy
   - Creating and deleting policies
   - Associating classes with a policy
   - Defining policy statements for a policy/class combination
3. Service
   - Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

NOTE: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

NOTE: Traffic to be processed by the DiffServ feature requires an IP header.

3.2.1 diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

Format `diffserv`

Mode Global Config

3.2.1.1 no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

Format `no diffserv`

Mode Global Config

3.3 DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class

match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

NOTE: Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is **class-map**.

3.3.1 class-map

This command defines a DiffServ class of type match-all. When used without any match condition, this command enters the class-map mode. The *<class-map-name>* is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

NOTE: The class-map-name 'default' is reserved and must not be used.

The class type of **match-all** indicates all of the individual match conditions must be true for a packet to be considered a member of the class.

NOTE: The CLI mode is changed to Class-Map Config when this command is successfully executed.

Format **class-map match-all** <*class-map-name*>

Mode Global Config

3.3.1.1 no class-map

This command eliminates an existing DiffServ class. The *<class-map-name>* is the name of an existing DiffServ class (The class name 'default' is reserved and is not allowed here). This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format **no class-map** <*class-map-name*>

Mode Global Config

3.3.2 class-map rename

This command changes the name of a DiffServ class. The **<***class-map-name***>** is the name of an existing DiffServ class. The **<***new-class-map-name***>** parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class (The *<class-map-name>* 'default' is reserved and must not be used here).

Default none

Format **class-map rename** <*class-map-name*> <*new-class-map-name*>

Mode Global Config

3.3.3 match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Default none

Format **match any**

Mode Class-Map Config

3.3.4 match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The *<refclassname>* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition. There is no default value.

Format **match class-map** *<refclassname>*

Mode Class-Map Config

NOTE:

- The parameters ***<refclassname>*** and *<class-map-name>* can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the *<refclassname>* class while the class is still referenced by any *<class-map-name>* fails.
- The combined match criteria of *<class-map-name>* and *<refclassname>* must be an allowed combination based on the class type.
- Any subsequent changes to the *<refclassname>* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

3.3.4.1 no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The *<refclassname>* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format **no match class-map** *<refclassname>*

Mode Class-Map Config

3.3.5 match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The *<ipaddr>* parameter specifies an IP address and *<ipmask>* specifies a subnet mask and must consist of a contiguous set of leading 1 bits.

Default none

Format **match dstip** *<ipaddr> <ipmask>*

Mode Class-Map Config

3.3.6 match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *<portkey>* is one of the supported port name keywords. The currently supported *<portkey>* values are: domain,

echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default none

Format **`match dstl4port`** *{<portkey> | <0-65535>}*

Mode Class-Map Config

3.3.7 match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The *<dscpval>* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

NOTE: The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default none

Format **`match ip dscp`** *<dscpval>*

Mode Class-Map Config

3.3.8 match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7.

NOTE: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default none

Format **`match ip precedence`** *<0-7>*

Mode Class-Map Config

3.3.9 match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of *<tosbits>* is a two-digit hexadecimal number from 00 to ff. The value of *<tosmask>* is a two-digit hexadecimal number from 00 to ff. The *<tosmask>* denotes the bit positions in *<tosbits>* that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a *<tosbits>* value of a0 (hex) and a *<tosmask>* of a2 (hex).

NOTE: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

NOTE: This "free form" version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

Default none

Format **`match ip tos`** *<tosbits> <tosmask>*

Mode Class-Map Config

3.3.10 match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for <protocol-name> is one of the supported protocol name keywords. The currently supported values are: `icmp`, `igmp`, `ip`, `tcp`, `udp`. A value of `ip` matches all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255.

NOTE: This command does not validate the protocol number value against the current list defined by IANA.

Default none

Format **`match protocol`** *{<protocol-name> | <0-255>}*

Mode Class-Map Config

3.3.11 match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The `<ipaddr>` parameter specifies an IP address. The `<ipmask>` parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default none

Format **`match srcip`** *<ipaddr> <ipmask>*

Mode Class-Map Config

3.3.12 match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for `<portkey>` is one of the supported port name keywords (listed below). The currently supported `<portkey>` values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default none

Format `match srcl4port` *{<portkey> | <0-65535>}*

Mode Class-Map Config

3.4 DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

NOTE: The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is `policy-map`.

3.4.1 assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The queueid is an integer from 0 to n-1, where n is the number of egress queues supported by the device.

Format `assign-queue` *<queueid>*

Mode Policy-Class-Map Config

Incompatibilities Drop

3.4.2 drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format `drop`

Mode Policy-Class-Map Config

Incompatibilities Assign Queue, Mark (all forms), Police

3.4.3 conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the

conform level are specified. The <class-map-name> parameter is the name of an existing Diffserv class map.

NOTE: This command may only be used after specifying a police command for the policy-class instance.

Format `conform-color` *<class-map-name>*

Mode Policy-Class-Map Config

3.4.4 class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The `<classname>` is the name of an existing DiffServ class.

NOTE: This command causes the specified policy to create a reference to the class definition.

NOTE: The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format `class` *<classname>*

Mode Policy-Map Config

3.4.4.1 no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. `<classname>` is the names of an existing DiffServ class.

NOTE: This command removes the reference to the class definition for the specified policy.

Format `no class` *<classname>*

Mode Policy-Map Config

3.4.5 mark cos

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Default 1

Format `mark-cos` *<0-7>*

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark IP DSCP, IP Precedence, Police

3.4.6 mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

The <dscpval> value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Format **mark ip-dscp** *<dscpval>*

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark CoS, Mark IP Precedence, Police

3.4.7 mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Format **mark ip-precedence** *<0-7>*

Mode Policy-Class-Map Config

Policy Type In

Incompatibilities Drop, Mark CoS, Mark IP DSCP, Police

3.4.8 police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop.

For set-dscp-transmit, a <dscpval> value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

Format **police-simple** *{<1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit}]}*

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark (all forms)

3.4.9 policy-map

This command establishes a new DiffServ policy. The <policyname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the in parameter.

NOTE: The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format **policy-map** *<policyname>* **in**

Mode Global Config

3.4.9.1 no policy-map

This command eliminates an existing DiffServ policy. The *<policyname>* parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format **no policy-map** *<policyname>*

Mode Global Config

3.4.10 policy-map rename

This command changes the name of a DiffServ policy. The *<policyname>* is the name of an existing DiffServ class. The *<newpolicyname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format **policy-map rename** *<policyname>* *<newpolicyname>*

Mode Global Config

3.5 DiffServ Service Commands

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

The CLI command root is **service-policy**.

3.5.1 service-policy

This command attaches a policy to an interface in the inbound direction. The *<policyname>* parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

NOTE: This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

NOTE: This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Format `service-policy in` <*policymapname*>

Modes Global Config
Interface Config

NOTE: Each interface can have one policy attached.

3.5.1.1 no service-policy

This command detaches a policy from an interface in the inbound direction. The <*policyname*> parameter is the name of an existing DiffServ policy.

NOTE: This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format `no service-policy in` <*policymapname*>

Modes Global Config
Interface Config

3.6 DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

3.6.1 show class-map

This command displays all configuration information for the specified class. The <*class-name*> is the name of an existing DiffServ class.

Format `show class-map` <*class-name*>

Modes Privileged EXEC
User EXEC

If the class-name is specified the following fields are displayed:

Class Name The name of this class.

Class Type A class type of ‘all’ means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.

Match Criteria The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.

Values The values of the Match Criteria.

If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed:

Class Name The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)

Class Type A class type of 'all' means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.

Ref Class Name The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

3.6.2 show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format `show diffserv`

Mode Privileged EXEC

DiffServ Admin mode The current value of the DiffServ administrative mode.

Class Table Size The current number of entries (rows) in the Class Table.

Class Table Max The maximum allowed entries (rows) for the Class Table.

Class Rule Table Size The current number of entries (rows) in the Class Rule Table.

Class Rule Table Max The maximum allowed entries (rows) for the Class Rule Table.

Policy Table Size The current number of entries (rows) in the Policy Table.

Policy Table Max The maximum allowed entries (rows) for the Policy Table.

Policy Instance Table Size Current number of entries (rows) in the Policy Instance Table.

Policy Instance Table Max Maximum allowed entries (rows) for the Policy Instance Table.

Policy Attribute Table Size Current number of entries (rows) in the Policy Attribute Table.

Policy Attribute Table Max Maximum allowed entries (rows) for the Policy Attribute Table.

Service Table Size The current number of entries (rows) in the Service Table.

Service Table Max The maximum allowed entries (rows) for the Service Table.

3.6.3 show policy-map

This command displays all configuration information for the specified policy. The *<policyname>* is the name of an existing DiffServ policy.

Format `show policy-map` *[policyname]*

Mode Privileged EXEC

If the Policy Name is specified the following fields are displayed:

Policy Name The name of this policy.

Type The policy type (Only inbound policy definitions are supported for this platform.)

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Assign Queue Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.

Class Name The name of this class.

Committed Burst Size (KB) The committed burst size, used in simple policing.

Committed Rate (Kbps) The committed rate, used in simple policing,

Conform Action The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.

Conform COS The CoS mark value if the conform action is set-cos-transmit.

Conform DSCP Value The DSCP mark value if the conform action is set-dscp-transmit.

Conform IP Precedence Value The IP Precedence mark value if the conform action is set-prec-transmit.

Drop Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.

Mark CoS The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.

Mark IP DSCP The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.

Mark IP Precedence The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.

Non-Conform Action The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.

Non-Conform COS The CoS mark value if the non-conform action is set-cos-transmit.

Non-Conform DSCP Value The DSCP mark value if the non-conform action is set-dscp-transmit.

Non-Conform IP Precedence Value The IP Precedence mark value if the non-conform action is set-prec-transmit.

Policing Style The style of policing, if any, used (simple).

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Policy Name The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)

Policy Type The policy type (Only inbound is supported).

Class Members List of all class names associated with this policy.

3.6.4 show diffserv service

This command displays policy service information for the specified interface and direction. The <slot/port> parameter specifies a valid slot/port number for the system.

Format **`show diffserv service`** <slot/port> **`in`**

Mode Privileged EXEC

DiffServ Admin Mode The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.

Interface Valid slot and port number separated by forward slashes.

Direction The traffic direction of this interface service.

Operational Status The current operational status of this DiffServ service interface.

Policy Name The name of the policy attached to the interface in the indicated direction.

Policy Details Attached policy details, whose content is identical to that described for the show policy-map *<policymapname>* command (content not repeated here for brevity).

3.6.5 show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format **`show diffserv service brief`** *[in]*

Mode Privileged EXEC

DiffServ Mode The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Interface Valid slot and port number separated by forward slashes.

Direction The traffic direction of this interface service.

OperStatus The current operational status of this DiffServ service interface.

Policy Name The name of the policy attached to the interface in the indicated direction.

3.6.6 show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The <slot/port> parameter specifies a valid interface for the system.

NOTE: This command is only allowed while the DiffServ administrative mode is enabled.

Format `show policy-map interface` <slot/port> *[in]*

Mode Privileged EXEC

Interface Valid slot and port number separated by forward slashes.

Direction The traffic direction of this interface service.

Operational Status The current operational status of this DiffServ service interface.

Policy Name The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Class Name The name of this class instance.

In Discarded Packets A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

3.6.7 show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format `show service-policy in`

Mode Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Interface Valid slot and port number separated by forward slashes.

Operational Status The current operational status of this DiffServ service interface.

Policy Name The name of the policy attached to the interface.

3.7 MAC Access Control List (ACL) Commands

This section describes the commands you use to configure MAC ACL settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- If you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

3.7.1 mac access-list extended

This command creates a MAC Access Control List (ACL) identified by <name>, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

NOTE: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format `mac access-list extended` <*name*>

Mode Global Config

3.7.1.1 no mac access-list extended

This command deletes a MAC ACL identified by <name> from the system.

Format `no mac access-list extended` <*name*>

Mode Global Config

3.7.2 mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The <name> parameter is the name of an existing MAC ACL. The <newname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name <newname> already exists.

Format `mac access-list extended rename` <*name*> <*newname*>

Mode Global Config

3.7.3 {deny | permit}

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

NOTE: The 'no' form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and re-specified.

NOTE: An implicit 'deny all' MAC rule always terminates the access list.

NOTE: Assign-queue attributes are configurable for a deny rule, but they have no operational effect.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *<ethertypekey>* values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Table 4.1. Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The vlan and cos parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <queue-id> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *assign-queue* parameter is valid only for a **permit** rule.

The *assign-queue* parameter is only valid for a **permit** rule.

NOTE: The special command form **{deny | permit} any any** is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

Format *{deny|permit} {<srcmac> | any} {<dstmac> | any} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [[log] [assign-queue <queue-id>]]*

Mode Mac-Access-List Config

3.7.4 mac access-group

This command attaches a specific MAC Access Control List (ACL) identified by *<name>* to an interface in a given direction. The *<name>* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not

specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

Format `mac access-group` *<name>* `in` *[sequence <1-4294967295>]*

Modes Global Config
Interface Config

3.7.4.1 no mac access-group

This command removes a MAC ACL identified by *<name>* from the interface in a given direction.

Format `no mac access-list` *<name>* `in`

Modes Global Config
Interface Config

3.7.5 show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the *[name]* parameter to identify a specific MAC ACL to display.

Format `show mac access-lists` *[name]*

Mode Privileged EXEC

Rule Number The ordered rule number identifier defined within the MAC ACL.

Action The action associated with each rule. The possible values are Permit or Deny.

Source MAC Address The source MAC address for this rule.

Destination MAC Address The destination MAC address for this rule.

Ethertype The Ethertype keyword or custom value for this rule.

VLAN ID The VLAN identifier value or range for this rule.

COS The COS (802.1p) value for this rule.

Log Displays when you enable logging for the rule.

Assign Queue The queue identifier to which packets matching this rule are assigned.

3.8 IP Access Control List (ACL) Commands

This section describes the commands you use to configure IP ACL settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- FASTPATH software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is 100, regardless of type.

- The maximum number of rules per IP ACL is hardware dependent.
- If you configure a MAC ACL on an interface, you cannot configure an IP ACL on the same interface.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored.

3.8.1 access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs. Table 4.2 describes the parameters for the **access-list** command.

IP Standard ACL:

Format **access-list** *<1-99> {deny | permit} {every | <srcip> <src-mask>} [log] [assign-queue <queue-id>]*

Mode Global Config

IP Extended ACL:

Format **access-list** *<100-199> {deny | permit} {every | icmp | igmp | ip | tcp | udp | <number>} {any | <srcip> <srcmask>} {any | eq {<portkey> | <0-65535>} | <dstip> <dstmask>} [eq {<portkey> | <0-65535>}] [{precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>}] [log] [assign-queue <queue-id>]*

Mode Global Config

Table 4.2. ACL Command Parameters

Parameter	Description
<1-99> or <100-199>	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
{deny | permit}	Specifies whether the IP ACL rule permits or denies an action. Note: Assign-queue attributes are configurable for a deny rule, but they have no operational effect.
every	Match every packet
{icmp | igmp | ip | tcp | udp | <number>}	Specifies the protocol to filter for an extended IP ACL rule.
<srcip> <srcmask>	Specifies a source IP address and source netmask for match condition of the IP ACL rule.

Table 4.2. ACL Command Parameters

Parameter	Description
[{eq {<portkey> | <0-65535>}]	Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the `<portkey>`, which can be one of the following keywords: `domain`, `echo`, `ftp`, `ftpdata`, `http`, `smtp`, `snmp`, `telnet`, `tftp`, and `www`. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
<dstip> <dstmask>	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
[precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters `dscp`, `precedence`, `tos/tosmask`.
[log]	Specifies that this rule is to be logged.
[assign-queue <queue-id>]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.

3.8.1.1 no access-list

This command deletes an IP ACL that is identified by the parameter `<accesslistnumber>` from the system. The range for `<accesslistnumber>` 1-99 for standard access lists and 100-199 for extended access lists.

Format **`no access-list`** *<accesslistnumber>*

Mode Global Config

3.8.2 ip access-group

This command attaches a specified IP ACL to one interface or to all interfaces.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Default none

Format **`ip access-group`** *<accesslistnumber>* **`in`** *[sequence <1-4294967295>]*

Modes Interface Config
Global Config

3.8.2.1 no ip access-group

This command removes a specified IP ACL from an interface.

Default none

Format `no ip access-group` <*accesslistnumber*> `in`

Mode Interface Config

3.8.3 acl-trapflags

This command enables the ACL trap mode.

Default disabled

Format `acl-trapflags`

Mode Global Config

3.8.3.1 no acl-trapflags

This command disables the ACL trap mode.

Format `no acl-trapflags`

Mode Global Config

3.8.4 show ip access-lists

This command displays an IP ACL <*accesslistnumber*> is the number used to identify the IP ACL.

Format `show ip access-lists` <*accesslistnumber*>

Mode Privileged EXEC

NOTE: Only the access list fields that you configure are displayed.

Rule Number The number identifier for each rule that is defined for the IP ACL.

Action The action associated with each rule. The possible values are Permit or Deny.

Match All Indicates whether this access list applies to every packet. Possible values are True or False.

Protocol The protocol to filter for this rule.

Source IP Address The source IP address for this rule.

Source IP Mask The source IP Mask for this rule.

Source L4 Port Keyword The source port for this rule.

Destination IP Address The destination IP address for this rule.

Destination IP Mask The destination IP Mask for this rule.

Destination L4 Port Keyword The destination port for this rule.

IP DSCP The value specified for IP DSCP.

IP Precedence The value specified IP Precedence.

IP TOS The value specified for IP TOS.

Log Displays when you enable logging for the rule.

Assign Queue The queue identifier to which packets matching this rule are assigned.

3.8.5 show access-lists

This command displays IP ACLs and MAC access control lists information for a designated interface and direction.

Format `show access-lists interface` <slot/port> `in`

Mode Privileged EXEC

ACL Type Type of access list (IP or MAC).

ACL ID Access List name for a MAC access list or the numeric identifier for an IP access list.

Sequence Number An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).



Chapter 4

Utility Commands

4. Utility Commands

This chapter describes the utility commands available in the CLI.

The FASTPATH Utility Commands chapter includes the following sections:

- 4.1 “Commands for update and startup Configuration“ on page 4 - 2
- 4.2 “ATCA commands“ on page 4 - 4
- 4.3 “System Information and Statistics Commands“ on page 4 - 5
- 4.4 “Logging Commands“ on page 4 - 19
- 4.5 “System Utility and Clear Commands“ on page 4 - 24
- 4.6 “Keying for Advanced Features“ on page 4 - 27
- 4.7 “Simple Network Time Protocol (SNTP) Commands“ on page 4 - 28
- 4.8 “DHCP Server Commands“ on page 4 - 32
- 4.9 “DHCP Filtering“ on page 4 - 42
- 4.10 “Serviceability Packet Tracing Commands“ on page 4 - 43

The commands in this chapter are in one of four functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

4.1 Commands for update and startup Configuration

The following commands are implemented to manipulate the Software images and configurations of the AT8402. The slot number (<slotnumber>) ranges from 0 - 9.

4.1.1 download ipmifw

This command copies an IPMI firmware image from URL and flashes the IPMC with the new image. If the flash process is interrupted or fails, the IPMC will automatically recover and use the previously installed image

Format `download ipmifw` *<url>*

Modes Privileged EXEC

4.1.2 download initrd

This command copies an initrd tgz (including kernel) from source-url and flash it to A or B location

Format `download initrd` *<url> {A | B}*

Modes Privileged EXEC

4.1.3 download frudata

This command restores the factory defaults for the FRU data.

Format `download frudata factory-default`

Modes Privileged EXEC

4.1.4 download fwum

This command updates the FWUM firmware. It downloads an FWUM firmware image from URL and flashes the FWUM with the new image. If the flash process is interrupted or fails, the FWUM will not recover gracefully and the board has to be repaired manually.

Use this command with extreme care. It is not field safe.

Do not interrupt the upgrade process.

Format `download fwum` *<url>*

Modes Privileged EXEC

4.1.5 download bootloader

This command loads a bootloader image into the second partition. It downloades a bootloader image from <url>. This image is used for the next boot process. If the download fails or the image is not correct (CRC error) the image in the first parttion is used.

Format `download bootloader` *<url>*

Modes Privileged EXEC

4.1.6 download amcipmifw

This command updates the IPMI firmware on an AMC. It downloads an IPMI firmware image from URL and flashes the MMC on the AMC with the new image. If the flash process is interrupted or fails, the MMC will automatically recover and use the previously installed image.

Format `download amcipmifw` *<url> <amcb1 | amcb2 | amcb3 | amcb4>*

Mode Privileged Exec

4.1.7 startupslot

This command configures the startup slot with the supplied values from the other slots. It will also check the configuration for consistency and flag any errors. The slot number (<slotnumber>) ranges from 0 - 9.

Format `startupslot` *<slotnumber>* `config` *<F,1-99>* `initrd` *<A,B>*

Mode Global Config

4.1.8 startupslot activate

This command sets the startup slot to active and will use this in all subsequent reboots. Using [once] at the end of the command will set the startup slot to be used once during the next restart. The start sequence will reset the startup slot to the previously installed one. This enables a try-once with automatic rollback in case of error.

Format `startupslot` *<slotnumber>* `activate` *[once]*

Mode Global Config

4.1.9 show startupconfig

This command shows either the installed system images or configuration files. For "startup" it shows the information about images and configuration files used at system startup. For "all" it shows all the information about installed images/files and the startup information.

Format `show startupconfig` *{initrd | startup | config | all}*

Modes Privileged EXEC

4.2 ATCA commands

4.2.1 set board sensor threshold

This command sets a new threashold value for a sensor. The <record-id> (of SDR) for a specific sensor is displayed by the related "show" command

Format `set board sensor threshold` *<record-id> <value-type> <value>*

Mode Privileged EXEC

<Value-type>

- lower-non-critical Set lower non-critical threshold value
- lower-critical Set lower critical threshold value
- lower-non-recover Set lower non-recoverable threshold value
- upper-non-critical Set upper non-critical threshold value
- upper-critical Set upper critical threshold value
- upper-non-recover Set upper non-recoverable threshold value

4.2.2 set board ipmi-controller debug

This command enables temporary IPMI controller serial debug output on the management serial console. .

Format `set board ipmi-controller debug` *{on | off}*

Mode Privileged EXEC

NOTE: Use this command with care as it may render the console useless until a full board reset is executed

4.2.3 set board device-id

This command sets the device ID for the board. The device ID is used in the management device locator sensor (show boardinfo sensors).

Format `set board device-id` *<string>*

Mode Privileged EXEC

4.2.4 set board fcap

This command enables or disables firmware capabilities.

- handle: If the handle capability is enabled, then the functionality of the hotswap-handle switch is disabled.

- pci-rst-hs: If the PCIE-reset capability is enabled, the PCIE infrastructure is set into reset if AMC in upstream-port is deactivated.
- pci-rst-cfg: If the PCIE-configuration setting is enabled, the PCIE switch will be reset if configuration is changed.

Format `set board fcap handle enable`
`set board fcap handle disable`
`set board fcap pci-rst-hs enable`
`set board fcap pci-rst-hs disable`
`set board fcap pci-rst-cfg enable`
`set board fcap pci-rst-cfg disable`

Mode Privileged EXEC

4.2.5 show atca ekeying

This command displays the current ekeying status together with admin mode and link status for all interfaces

Format `show atca ekeying all`

Mode Privileged EXEC

4.2.6 ekeying (interface)

This command enables the ekeying for one port. Default is enabled.

Format `ekeying`

Mode Interface Config

4.2.6.1 no ekeying (interface)

This command disables the ekeying for one port. Default is enabled.

Format `no ekeying`

Mode Interface Config

4.2.7 set board bootcycle

This command activates/deactivates a bootcycle-detection and (if activated) sets the related parameters. Parameter ‘none’ deactivates the bootcycle detection. Parameters ‘event’ and ‘pwr-down’ activate the bootcycle detection and execute an action if the number of <cyles>, checked in <interval> seconds, is reached. The executed action is the generation of an event and additionally for ‘pwr-down’ switch off the Power-PC.

Format `set board bootcycle none`
`set board bootcycle event` *<interval> <cycles>*
`set board bootcycle pwr-down` *<interval> <cycles>*

Mode Priviliged EXEC

4.3 System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

4.3.1 show arp switch

This command displays the contents of the IP stack's Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces - network or service ports. ARP entries associated with routing interfaces are not listed.

Format `show arp switch`

Mode Privileged EXEC

IP Address IP address of the management interface or another device on the management network.

MAC Address Hardware MAC address of that device.

Interface For a service port the output is *Management*. For a network port, the output is the slot/port of the physical interface.

4.3.2 show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

Format `show eventlog`

Mode Privileged EXEC

File The file in which the event originated.

Line The line number of the event

Task Id The task ID of the event.

Code The event code.

Time The time this event occurred.

NOTE: Event log information is retained across a switch reset.

4.3.3 show hardware

This command displays inventory information for the switch.

NOTE: The `show version` command and the `show hardware` command display the same information. In future releases of the software, the `show hardware` command will not be available. For a description of the command output, see 4.3.4 "show version" on page 4 - 6.

Format `show hardware`

Mode Privileged EXEC

4.3.4 show version

This command displays inventory information for the switch.

NOTE: The `show version` command will replace the `show hardware` command in future releases of the software.

Format `show version`

Mode Privileged EXEC

Switch Description Text used to identify the product name of this switch.

Machine Type The machine model as defined by the Vital Product Data.

Machine Model The machine model as defined by the Vital Product Data.

Serial Number The unique box serial number for this switch.

FRU Number The field replaceable unit number.

Part Number Manufacturing part number.

Maintenance Level Hardware changes that are significant to software.

Manufacturer Manufacturer descriptor field.

Burned in MAC Address Universally assigned network address.

Software Version The release.version.revision number of the code currently running on the switch.

Operating System The operating system currently running on the switch.

Network Processing Device The type of the processor microcode.

Additional Packages The additional packages incorporated into this system.

4.3.5 show interface

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

Format `show interface` *{*<slot/port> | *switchport}*

Mode Privileged EXEC

The display parameters, when the argument is <slot/port>, is as follows:

Packets Received Without Error The total number of packets (including broadcast packets and multicast packets) received by the processor.

Packets Received With Error The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Broadcast Packets Received The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Transmitted Without Error The total number of packets transmitted out of the interface.

Transmit Packets Errors The number of outbound packets that could not be transmitted because of errors.

Collisions Frames The best estimate of the total number of collisions on this Ethernet segment.

Time Since Counters Last Cleared The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is “switchport” is as follows:

Broadcast Packets Received The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received With Error The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Packets Transmitted Without Error The total number of packets transmitted out of the interface.

Broadcast Packets Transmitted The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packet Errors The number of outbound packets that could not be transmitted because of errors.

Address Entries Currently In Use The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.

VLAN Entries Currently In Use The number of VLAN entries presently occupying the VLAN table.

Time Since Counters Last Cleared The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

4.3.6 show interface ethernet

This command displays detailed statistics for a specific interface or for all CPU traffic based upon the argument.

Format `show interface ethernet` *{*<slot/port> | *switchport}*

Mode Privileged EXEC

The when you specify a value for <slot/port>, the command displays the following information:

Packets Received

Total Packets Received (Octets) - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.

Packets Received 64 Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Received 65-127 Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 128-255 Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 256-511 Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 512-1023 Octets - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 1024-1518 Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received > 1522 Octets - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Packets RX and TX 64 Octets - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).

Packets RX and TX 65-127 Octets - The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets RX and TX 128-255 Octets - The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets RX and TX 256-511 Octets - The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets RX and TX 512-1023 Octets - The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Packets RX and TX 1024-1518 Octets - The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Packets RX and TX 1519-1522 Octets - The total number of packets (including bad packets) received and transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

Packets RX and TX 1523-2047 Octets - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.

Packets RX and TX 2048-4095 Octets - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.

Packets RX and TX 4096-9216 Octets - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.

Packets Received Successfully

Total Packets Received Without Error - The total number of packets received that were without errors.

Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received with MAC Errors

Total - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Jabbers Received - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Fragments/Undersize Received - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).

Alignment Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.

Rx FCS Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

Overruns - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Received Packets Not Forwarded

Total - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process.

Local Traffic Frames - The total number of frames dropped in the forwarding process because the destination address was located off of this port.

802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Unacceptable Frame Type - The number of frames discarded from this port due to being an unacceptable frame type.

Multicast Tree Viable Discards - The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.

Reserved Address Discards - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.

Broadcast Storm Recovery - The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.

CFI Discards - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.

Upstream Threshold - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Packets Transmitted Octets

Total Bytes - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. -----

Packets Transmitted 64 Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 65-127 Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 128-255 Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 256-511 Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 512-1023 Octets - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 1024-1518 Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Max Frame Size - The maximum size of the Info (non-MAC) field that this port will receive or transmit.

Packets Transmitted Successfully

Total - The number of frames that have been transmitted by this port to its segment.

Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Errors

Total Errors - The sum of Single, Multiple, and Excessive Collisions.

Tx FCS Errors - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

Oversized - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.

Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Transmit Discards

Total Discards - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.

Single Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Multiple Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Excessive Collisions - A count of frames for which transmission on a particular interface fails due to excessive collisions.

Port Membership Discards - The number of frames discarded on egress for this port due to egress filtering being enabled.

Protocol Statistics

802.3x Pause Frames Transmitted - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE

operation. This counter does not increment when the interface is operating in half-duplex mode.

GVRP PDUs Received - The count of GVRP PDUs received in the GARP layer.

GVRP PDUs Transmitted - The count of GVRP PDUs transmitted from the GARP layer.

GVRP Failed Registrations - The number of times attempted GVRP registrations could not be completed.

GMRP PDUs Received - The count of GMRP PDU's received in the GARP layer.

GMRP PDUs Transmitted - The count of GMRP PDU's transmitted from the GARP layer.

GMRP Failed Registrations - The number of times attempted GMRP registrations could not be completed.

STP BPDUs Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received - Spanning Tree Protocol Bridge Protocol Data Units received

RST BPDUs Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RSTP BPDUs Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received

MSTP BPDUs Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received

Dot1x Statistics

EAPOL Frames Received - The number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.

Time Since Counters Last Cleared The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

If you use the *switchport* keyword, the following information appears:

Octets Received The total number of octets of data received by the processor (excluding framing bits but including FCS octets).

Total Packets Received Without Error The total number of packets (including broadcast packets and multicast packets) received by the processor.

Unicast Packets Received The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Receive Packets Discarded The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Octets Transmitted The total number of octets transmitted out of the interface, including framing characters.

Packets Transmitted without Errors The total number of packets transmitted out of the interface.

Unicast Packets Transmitted The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packets Discarded The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Most Address Entries Ever Used The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.

Address Entries in Use The number of Learned and static entries in the Forwarding Database Address Table for this switch.

Maximum VLAN Entries The maximum number of Virtual LANs (VLANs) allowed on this switch.

Most VLAN Entries Ever Used The largest number of VLANs that have been active on this switch since the last reboot.

Static VLAN Entries The number of presently active VLAN entries on this switch that have been created statically.

Dynamic VLAN Entries The number of presently active VLAN entries on this switch that have been created by GVRP registration.

VLAN Deletes The number of VLANs on this switch that have been created and then deleted since the last reboot.

Time Since Counters Last Cleared The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

4.3.7 show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter *all* or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the *count* parameter to view summary information about the forwarding database table. Use the *interface* <slot/port> parameter to view MAC addresses on a specific interface. Use the *vlan* <*vlan_id*> parameter to display information about MAC addresses on a specified VLAN.

Format **`show mac-addr-table`** *[{<macaddr> <vlan_id> | all | count | interface* <slot/port> | *vlan <vlan_id>}]*

Mode Privileged EXEC

The following information displays if you do not enter a parameter, the keyword all, or the MAC address and VLAN ID. If you enter *vlan* <*vlan_id*>, only the Mac Address, Interface, and Status fields appear.

Mac Address A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.

Interface The port through which this address was learned.

Interface Index This object indicates the ifIndex of the interface table entry associated with this port.

Status The status of this entry. The meanings of the values are:

Static—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned.

Learned—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.

Management—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing.

Self—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address).

GMRP Learned—The value of the corresponding was learned via GMRP and applies to Multicast.

Other—The value of the corresponding instance does not fall into one of the other categories.

If you enter the *interface* <slot/port> parameter, in addition to the MAC Address and Status fields, the following field appears:

VLAN ID The VLAN on which the MAC address was learned.

The following information displays if you enter the *count* parameter:

Dynamic Address count Number of MAC addresses in the forwarding database that were automatically learned.

Static Address (User-defined) count Number of MAC addresses in the forwarding database that were manually entered by a user.

Total MAC Addresses in use Number of MAC addresses currently in the forwarding database.

Total MAC Addresses available Number of MAC addresses the forwarding database can handle.

4.3.8 show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the *[all]* option.

NOTE: Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional <*scriptname*> is provided with a file name extension of ".scr", the output is redirected to a script file.

NOTE: If you issue the **`show running-config`** command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

Format **`show running-config`** *[all | <scriptname>]*

Mode Privileged EXEC

4.3.9 show sysinfo

This command displays switch information.

Format **`show sysinfo`**

Mode Privileged EXEC

Switch Description Text used to identify this switch.

System Name Name used to identify the switch.The factory default is blank. To configure the system name, see 5.6.1 "snmp-server" on page 5 - 15.

System Location Text used to identify the location of the switch. The factory default is blank. To configure the system location, see 5.6.1 "snmp-server" on page 5 - 15.

System Contact Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see 5.6.1 "snmp-server" on page 5 - 15.

System ObjectID The base object ID for the switch's enterprise MIB.

System Up Time The time in days, hours and minutes since the last switch reboot.

MIBs Supported A list of MIBs supported by this agent.

4.3.10 show tech-support

Use the **show tech-support** command to display system and configuration information when you contact technical support. The output of the **show tech-support** command combines the output of the following commands:

- **show version**
- **show sysinfo**
- **show port all**
- **show logging**
- **show event log**
- **show logging buffered**
- **show trap log**
- **show running config**

Format **show tech-support**

Mode Privileged EXEC

4.3.11 show boardinfo post-status

This command displays the system power on self test status.

Format **show boardinfo post-status system**

Mode Privileged EXEC

4.3.12 show boardinfo sensors

This command displays the current sensor readings. It can either display a compressed list of all sensors or display full readings for a specified sensor. The <record-id> (of SDR) for a specific sensor is displayed in the compressed list

Format **show boardinfo sensors** *{<record-id> | brief}*

Mode Privileged EXEC

NOTE: It might take a while to get an output of the *"show boardinfo sensors brief"* command

4.3.13 show boardinfo event-log

This command displays the event log of the board management controller. It can either display a summary ("info") or a list of all existing event-log records, a list with most recent records or a single record. The <record-id> (of SEL) is displayed in the list of records.

Format **show boardinfo event-log** *{info | list [last <nr-of-most-recent-entries> | <record-id>]}*

Mode Privileged EXEC

NOTE: It might take a while to get an output of the *"show boardinfo event-log list"* command

4.3.14 show boardinfo update-status

This command displays the status of the firmware update process for the IPMI controller.

Format `show boardinfo update-status`

Mode Privileged EXEC

4.3.15 show boardinfo version

This command displays hardware and software revision information. This includes serial-numbers, software and hardware revisions as applicable.

Format `show boardinfo version`

Mode Privileged EXEC

Version information included

- Base board serial number
- Basic product identification (product number)
- IPMC firmware version and release
- FWUM firmware version
- System U-boot version and release
- System kernel version and release
- System OS release
- FASTPATH version and release
- Base board revision
- CPLD revision
- Broadcom Silicon revision
- Processor CPU
- Processor clock
- Flash size

4.3.16 show boardinfo address

This command displays the global address info of the board.

Format `show boardinfo address`

Mode Privileged EXEC

4.3.17 show boardinfo fru

This command displays various FRU (field replaceable unit) related information.

Format `show boardinfo fru` *{product-info | board-info | multi-record | custom-area | all}*

Mode Privileged EXEC

4.3.18 show boardinfo ipmidev

This command displays the IPMI device information. This consists of Firmware Revision, IPMI version, Manufacturer and Product ID.

Format `show boardinfo ipmidev`

Mode Privileged EXEC

4.3.19 show boardinfo led

This command displays the LED status.

Format `show boardinfo led`

Mode Privileged EXEC

4.3.20 show boardinfo fcap

This command shows the user changeable firmware capabilities.

Format `show boardinfo fcap`

Mode Privileged EXEC

4.3.21 show boardinfo amc connection

This command displays the connections to an AMC carrier.

Format `show boardinfo amc connection` *{amcb1 | amcb2 | amcb3 | amcb4}*
`show boardinfo amc connection all`

Mode Privileged EXEC

4.3.22 show boardinfo amc fru

This command displays various FRU (field replaceable unit) related information (or all FRU information) for a specified AMC.

Format `show boardinfo amc fru product-info` *{amcb1 | amcb2 | amcb3 | amcb4}*
`show boardinfo amc fru board-info` *{amcb1 | amcb2 | amcb3 | amcb4}*
`show boardinfo amc fru multi-record` *{amcb1 | amcb2 | amcb3 | amcb4}*
`show boardinfo amc fru custom-area` *{amcb1 | amcb2 | amcb3 | amcb4}*
`show boardinfo amc fru all` *{amcb1 | amcb2 | amcb3 | amcb4}*

Mode Privileged EXEC

4.3.23 show boardinfo amc ipmidev

This command displays the IPMI device information for a specified AMC. This includes Firmware Revision, IPMI version, Manufacturer and Product ID.

Format `show boardinfo amc ipmidev` *{amcb1 | amcb2 | amcb3 | amcb4}*

Mode Privileged EXEC

4.3.24 show boardinfo bootcycle

This command displays whether a bootcycle-detection is activated and (if activated) the related parameters.

Format `show boardinfo bootcycle`

Mode Priviliged EXEC

4.4 Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

4.4.1 logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

Default disabled; critical when enabled

Format `logging buffered`

Mode Global Config

4.4.1.1 no logging buffered

This command disables logging to in-memory log.

Format `no logging buffered`

Mode Global Config

4.4.2 logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default enabled

Format `logging buffered wrap`

Mode Privileged EXEC

4.4.2.1 no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format `no logging buffered wrap`

Mode Privileged EXEC

4.4.3 logging cli-command

This command enables the CLI command logging feature, which enables the FASTPATH software to log all CLI commands issued on the system.

Default `enabled`

Format `logging cli-command`

Mode `Global Config`

4.4.3.1 no logging cli-command

This command disables the CLI command Logging feature.

Format `no logging cli-command`

Mode `Global Config`

4.4.4 logging console

This command enables logging to the console. You can specify the <*severitylevel*> value as either an integer from 0 to 7 or symbolically through one of the following

keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default disabled; critical when enabled

Format **logging console** *[severitylevel]*

Mode Global Config

4.4.4.1 no logging console

This command disables logging to the console.

Format **no logging console**

Mode Global Config

4.4.5 logging host

This command enables logging to a host. You can configure up to eight hosts. The <*ipaddr*> is the IP address of the logging host. The <*port*> value is a port number from 1 to 65535. You can specify the <*severitylevel*> value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default port—514
level—critical (2)

Format **logging host** <*ipaddr*> *[<port>][<severitylevel>]*

Mode Global Config

4.4.6 logging host remove

This command disables logging to host. See 4.4.11 “show logging hosts“ on page 4 - 23 for a list of host indexes.

Format **logging host remove** <*hostindex*>

Mode Global Config

4.4.7 logging port

This command sets the local port number of the LOG client for logging messages. The <*portid*> can be in the range from 1 to 65535.

Default 514

Format **logging port** <*portid*>

Mode Global Config

4.4.7.1 no logging port

This command resets the local logging port to the default.

Format **no logging port**

Mode Global Config

4.4.8 logging syslog

This command enables syslog logging. The <*portid*> parameter is an integer with a range of 1-65535.

Default disabled

Format `logging syslog` *[port <portid>]*

Mode Global Config

4.4.8.1 no logging syslog

This command disables syslog logging.

Format `no logging syslog`

Mode Global Config

4.4.9 show logging

This command displays logging configuration information.

Format `show logging`

Mode Privileged EXEC

Logging Client Local Port Port on the collector/relay to which syslog messages are sent.

CLI Command Logging Shows whether CLI Command logging is enabled.

Console Logging Shows whether console logging is enabled.

Console Logging Severity Filter The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.

Buffered Logging Shows whether buffered logging is enabled.

Syslog Logging Shows whether syslog logging is enabled.

Log Messages Received Number of messages received by the log process. This includes messages that are dropped or ignored.

Log Messages Dropped Number of messages that could not be processed due to error or lack of resources.

Log Messages Relayed Number of messages sent to the collector/relay.

4.4.10 show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format `show logging buffered`

Mode Privileged EXEC

Buffered (In-Memory) Logging Shows whether the In-Memory log is enabled or disabled.

Buffered Logging Wrapping Behavior The behavior of the In Memory log when faced with a log full situation.

Buffered Log Count The count of valid entries in the buffered log.

4.4.11 show logging hosts

This command displays all configured logging hosts.

Format `show logging hosts`

Mode Privileged EXEC

Host Index (Used for deleting hosts)

IP Address IP address of the logging host.

Severity Level The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).

Port Displays the server port number, which is the port on the local host from which syslog messages are sent.

Host Status The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

4.4.12 show logging traplogs

This command displays SNMP trap events and statistics.

Format `show logging traplogs`

Mode Privileged EXEC

Number of Traps Since Last Reset The number of traps since the last boot.

Trap Log Capacity The number of traps the system can retain.

Number of Traps Since Log Last Viewed The number of new traps since the command was last executed.

Log The log number.

System Time Up How long the system had been running at the time the trap was sent.

Trap The text of the trap message.

4.4.13 clear board event-log

This command deletes all event-log records

Format `clear board event-log`

Mode Privileged EXEC

4.4.14 show logging backtrace

This command displays the backtrace file last created. A backtrace file is created when the application stops unexpectedly.

Format `show logging backtrace`

Modes Privileged EXEC

4.4.15 show logging diag-report

This command displays the results of the last diagnostic run. The diagnostic results file is created by a diagnostic run.

Format `show logging diag-report`

Mode Privileged Exec

4.5 System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

4.5.1 traceroute

Use the **`traceroute`** command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The *<ipaddr>* value should be a valid IP address. The *[<port>]* value should be a valid decimal integer in the range of 0 (zero) to 65535. The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. The default value is 33434.

Format **`traceroute`** *<ipaddr> [<port>]*

Mode Privileged EXEC

4.5.2 clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter **`y`**, you automatically reset current configuration on the switch to the default values. It does not reset the switch.

Format **`clear config`**

Mode Privileged EXEC

4.5.3 clear counters

This command clears the statistics for a specified <slot/port>, for all the ports, or for the entire switch based upon the argument.

Format **`clear counters`** *{*<slot/port> | *all}*

Mode Privileged EXEC

4.5.4 clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format **`clear igmpsnooping`**

Mode Privileged EXEC

4.5.5 clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format **`clear pass`**

Mode Privileged EXEC

4.5.6 clear port-channel

This command clears all port-channels (LAGs).

Format `clear port-channel`

Mode Privileged EXEC

4.5.7 clear traplog

This command clears the trap log.

Format `clear traplog`

Mode Privileged EXEC

4.5.8 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format `clear vlan`

Mode Privileged EXEC

4.5.9 enable passwd

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of eight alphanumeric characters. The password is case sensitive.

Format `enable passwd`

Mode User EXEC

4.5.10 logout

This command closes the current telnet connection or resets the current serial connection.

NOTE: Save configuration changes before logging out.

Format `logout`

Modes Privileged EXEC
User EXEC

4.5.11 set bootstopkey

This command sets the bootstop key. With this key the booting process can be stopped. The key name is “stop”. This is the default setting.

Format `set bootstopkey`

Mode Privileged EXEC

4.5.11.1 no set bootstopkey

This command resets the bootstop key. The boot process can not be interrupted.

Format `no set bootstopkey`

Mode Privileged EXEC

4.5.12 ping

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. You can ping the switch from any IP workstation the switch is connected to through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

Format `ping` <*ipaddr*>

Modes Privileged EXEC
User EXEC

4.5.13 quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format `quit`

Modes Privileged EXEC
User EXEC

4.5.14 reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format `reload`

Mode Privileged EXEC

4.5.15 copy

The `copy` command uploads and downloads files to and from the switch. Upload and download files from a server by using TFTP or Xmodem.

Format `copy` <*source*> <*destination*>

Mode Privileged EXEC

Replace the <*source*> and <*destination*> parameters with the options in Table 4.1. For the <*url*> source or destination, use one of the following values:

{xmodem | tftp://<ipaddr>/<filepath>/<filename>}

For TFTP, the <*ipaddr*> parameter is the IP address of the server, <*filepath*> is the path to the file, and <*filename*> is the name of the file you want to upload or download.

Table 4.1. Copy Parameters

Source	Destination	Description
nvram:clibanner	*<url>*	Copies the CLI banner to a server.
nvram:errorlog	*<url>*	Copies the error log file to a server.
nvram:log	*<url>*	Copies the log file to a server.
nvram:script <script-name>	*<url>*	Copies a specified configuration script file to a server.
nvram:startup-config	*<url>*	Copies the startup configuration to a server.
nvram:traplog	*<url>*	Copies the trap log file to a server.
system:running-config	*nvram:startup-config*	Saves the running configuration to nvram.
<url>	*nvram:clibanner*	Downloads the CLI banner to the system.
<url>	*nvram:script <destfilename>*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
<url>	*nvram:sshkey-dsa*	Downloads an SSH key file. For more information, see 5.4 “Secure Shell (SSH) Command“ on page 5 - 10.
<url>	*nvram:sshkey-rsa1*	Downloads an SSH key file.
<url>	*nvram:sshkey-rsa2*	Downloads an SSH key file.
<url>	*nvram:startup-config*	Downloads the startup configuration file to the system.

4.6 Keying for Advanced Features

This section describes the commands you use to enter the licence key to access advanced features. You cannot access the advanced features without a valid license key.

4.6.1 license advanced

This command enables a particular feature. This command also enables the corresponding show commands for a feature.

NOTE: If the feature is enabled, the feature is visible in the output of the **`show running-config`** command. The *<key>* parameter specifies the hexadecimal key for the feature.

Default none

Format **`license advanced`** *<key>*

Mode Privileged EXEC

4.6.1.1 no license advanced

This command disables a particular feature. This command also disables the corresponding show commands. The <*key*> parameter specifies the hexadecimal key for the feature.

Format `no license advanced` <*key*>

Mode Privileged EXEC

4.6.2 show key-features

This command displays the enabled or disabled status for all keyable features.

Format `show key-features`

Modes Privileged EXEC
User EXEC

Function This is the name of the keyable component or feature.

Status Enabled or disabled.

4.7 Simple Network Time Protocol (SNTP) Commands

This section describes the commands you use to automatically configure the system time and date by using SNTP.

4.7.1 sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where <poll-interval> can be a value from 6 to 16.

Default 6

Format `sntp broadcast client poll-interval` <*poll-interval*>

Mode Global Config

4.7.1.1 no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Format `no sntp broadcast client poll-interval`

Mode Global Config

4.7.2 sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default disabled

Format `sntp client mode` *[broadcast | unicast]*

Mode Global Config

4.7.2.1 no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format `no sntp client mode`

Mode Global Config

4.7.3 sntp client port

This command sets the SNTP client port id to a value from 1-65535.

Default 123

Format `sntp client port` *<portid>*

Mode Global Config

4.7.3.1 no sntp client port

This command resets the SNTP client port back to its default value.

Format `no sntp client port`

Mode Global Config

4.7.4 sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where <poll-interval> can be a value from 6 to 16.

Default 6

Format `sntp unicast client poll-interval` *<poll-interval>*

Mode Global Config

4.7.4.1 no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-interval`

Mode Global Config

4.7.5 sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

Default 5

Format `sntp unicast client poll-timeout` *<poll-timeout>*

Mode Global Config

4.7.5.1 no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-timeout`

Mode Global Config

4.7.6 sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

Default 1

Format `sntp unicast client poll-retry` *<poll-retry>*

Mode Global Config

4.7.6.1 no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-retry`

Mode Global Config

4.7.7 sntp multicast client poll-interval

This command will set the poll interval for SNTP multicast clients in seconds as a power of two where *<poll-interval>* can be a value from 6 to 16.

Default 6

Format `sntp multicast client poll-interval` *<poll-interval>*

Mode Global Config

4.7.7.1 no sntp multicast client poll-interval

This command resets the poll interval for SNTP multicast clients to its default value.

Format `no sntp multicast client poll-interval`

Mode Global Config

4.7.8 sntp server

This command configures an SNTP server (a maximum of three). The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

Format `sntp server` *<ipaddress> [<priority> [<version> [<portid>]]]*

Mode Global Config

4.7.8.1 no sntp server

This command deletes an server from the configured SNTP servers.

Format `no sntp server remove` *<ipaddress>*

Mode Global Config

4.7.9 show sntp

This command is used to display SNTP settings and status.

Format `show sntp`

Mode Privileged EXEC

Last Update Time Time of last clock update.

Last Attempt Time Time of last transmit query (in unicast mode).

Last Attempt Status Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).

Broadcast Count Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

Multicast Count Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot

4.7.10 show sntp client

This command is used to display SNTP client settings.

Format `show sntp client`

Mode Privileged EXEC

Client Supported Modes Supported SNTP Modes (Broadcast, Unicast, or Multicast).

SNTP Version The highest SNTP version the client supports

Port SNTP Client Port

Client Mode Configured SNTP Client Mode

4.7.11 show sntp server

This command is used to display SNTP server settings and configured servers.

Format `show sntp server`

Mode Privileged EXEC

Server IP Address IP address of configured SNTP Server

Server Type Address Type of Server.

Server Stratum Claimed stratum of the server for the last received valid packet.

Server Reference ID Reference clock identifier of the server for the last received valid packet.

Server Mode SNTP Server mode.

Server Maximum Entries Total number of SNTP Servers allowed.

Server Current Entries Total number of SNTP configured.

For each configured server:

IP Address IP address of configured SNTP Server.

Address Type Address Type of configured SNTP server.

Priority IP priority type of the configured server.

Version SNTP Version number of the server. The protocol version used to query the server in unicast mode.

Port Server Port Number

Last Attempt Time Last server attempt time for the specified server.

Last Update Status Last server attempt status for the server.

Total Unicast Requests Number of requests to the server.

Failed Unicast Requests Number of failed requests from server.

4.8 DHCP Server Commands

This section describes the commands you to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

4.8.1 ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode.

Default none

Format `ip dhcp pool` <*name*>

Mode Global Config

4.8.1.1 no ip dhcp pool

This command removes the DHCP address pool. The name should be previously configured pool name.

Format `no ip dhcp pool` <*name*>

Mode Global Config

4.8.2 client-identifier

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique-identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, Assigned Numbers for a list of media type codes.

Default none

Format `client-identifier` <*uniqueidentifier*>

Mode DHCP Pool Config

4.8.2.1 no client-identifier

This command deletes the client identifier.

Format `no client-identifier`

Mode DHCP Pool Config

4.8.3 client-name

This command specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

Default none

Format `client-name` *<name>*

Mode DHCP Pool Config

4.8.3.1 no client-name

This command removes the client name.

Format `no client-name`

Mode DHCP Pool Config

4.8.4 default-router

This command specifies the default router list for a DHCP client. {*address1, address2... address8*} are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default none

Format `default-router` *<address1> [<address2>....<address8>]*

Mode DHCP Pool Config

4.8.4.1 no default-router

This command removes the default router list.

Format `no default-router`

Mode DHCP Pool Config

4.8.5 dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default none

Format `dns-server` *<address1> [<address2>....<address8>]*

Mode DHCP Pool Config

4.8.5.1 no dns-server

This command removes the DNS Server list.

Format `no dns-server`

Mode DHCP Pool Config

4.8.6 hardware-address

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

Default ethernet

Format **`hardware-address`** *<hardwareaddress> <type>*

Mode DHCP Pool Config

4.8.6.1 no hardware-address

This command removes the hardware address of the DHCP client.

Format **`no hardware-address`**

Mode DHCP Pool Config

4.8.7 host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32

Default none

Format **`host`** *<address> [{<mask> | <prefix-length>}]*

Mode DHCP Pool Config

4.8.7.1 no host

This command removes the IP address of the DHCP client.

Format **`no host`**

Mode DHCP Pool Config

4.8.8 lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If you specify *infinite*, the lease is set for 60 days. You can also specify a lease duration. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 1439. *Minutes* is an integer from 0 to 86399.

Default 1 (day)

Format **`lease`** *[{<days> [<hours>] [<minutes>] | infinite}]*

Mode DHCP Pool Config

4.8.8.1 no lease

This command restores the default value of the lease time for DHCP Server.

Format `no lease`

Mode DHCP Pool Config

4.8.9 network (DHCP Pool Config)

Use this command to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

Default none

Format `network` *<networknumber> [{<mask> | <prefixlength>}]*

Mode DHCP Pool Config

4.8.9.1 no network

This command removes the subnet number and mask.

Format `no network`

Mode DHCP Pool Config

4.8.10 bootfile

The command specifies the name of the default boot image for a DHCP client. The *<filename>* specifies the boot image file.

Format `bootfile` *<filename>*

Mode DHCP Pool Config

4.8.10.1 no bootfile

This command deletes the boot image name.

Format `no bootfile`

Mode DHCP Pool Config

4.8.11 domain-name

This command specifies the domain name for a DHCP client. The *<domain>* specifies the domain name string of the client.

Default none

Format `domain-name` *<domain>*

Mode DHCP Pool Config

4.8.11.1 no domain-name

This command removes the domain name.

Format `no domain-name`

Mode DHCP Pool Config

4.8.12 netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Default none

Format `netbios-name-server` *<address> [<address2>...<address8>]*

Mode DHCP Pool Config

4.8.12.1 no netbios-name-server

This command removes the NetBIOS name server list.

Format `no netbios-name-server`

Mode DHCP Pool Config

4.8.13 netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients.type Specifies the NetBIOS node type. Valid types are:

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed
- h-node—Hybrid (recommended)

Default none

Format `netbios-node-type` *<type>*

Mode DHCP Pool Config

4.8.13.1 no netbios-node-type

This command removes the NetBIOS node Type.

Format `no netbios-node-type`

Mode DHCP Pool Config

4.8.14 next-server

This command configures the next server in the boot process of a DHCP client.The *<address>* parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

Default inbound interface helper addresses

Format `next-server` *<address>*

Mode DHCP Pool Config

4.8.14.1 no next-server

This command removes the boot server list.

Format `no next-server`

Mode DHCP Pool Config

4.8.15 option

The `option` command configures DHCP Server options. The *<code>* parameter specifies the DHCP option code and ranges from 1-254. The *<ascii string>* parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The *hex <string>* parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, a3.4f.22.0c), colon (for example, a3:4f:22:0c), or white space (for example, a3 4f 22 0c).

Default none

Format `option` *<code> {ascii string | hex <string1> [<string2>...<string8>] | ip <address1> [<address2>...<address8>]}*

Mode DHCP Pool Config

4.8.15.1 no option

This command removes the DHCP Server options. The *<code>* parameter specifies the DHCP option code.

Format `no option` *<code>*

Mode DHCP Pool Config

4.8.16 ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default none

Format `ip dhcp excluded-address` *<lowaddress> [highaddress]*

Mode Global Config

4.8.16.1 no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format `no ip dhcp excluded-address` *<lowaddress> [highaddress]*

Mode Global Config

4.8.17 ip dhcp ping packets

Use this command to specify the number, in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

Default 2

Format `ip dhcp ping packets` *<0,2-10>*

Mode Global Config

4.8.17.1 no ip dhcp ping packets

This command prevents the server from pinging pool addresses and sets the number of packets to 0.

Default 0

Format `no ip dhcp ping packets`

Mode Global Config

4.8.18 service dhcp

This command enables the DHCP server.

Default disabled

Format `service dhcp`

Mode Global Config

4.8.18.1 no service dhcp

This command disables the DHCP server.

Format `no service dhcp`

Mode Global Config

4.8.19 ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

Default disabled

Format `ip dhcp bootp automatic`

Mode Global Config

4.8.19.1 no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

Format `no ip dhcp bootp automatic`

Mode Global Config

4.8.20 ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default enabled

Format `ip dhcp conflict logging`

Mode Global Config

4.8.20.1 no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format `no ip dhcp conflict logging`

Mode Global Config

4.8.21 clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If "*" is specified, the bindings corresponding to all the addresses are deleted. *<address>* is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format `clear ip dhcp binding` *{<address> | *}*

Mode Privileged EXEC

4.8.22 clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format `clear ip dhcp server statistics`

Mode Privileged EXEC

4.8.23 clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If the asterisk (*) character is used as the address parameter.

Default none

Format `clear ip dhcp conflict` *{<address> | *}*

Mode Privileged EXEC

4.8.24 show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format `show ip dhcp binding` *[<address>]*

Modes Privileged EXEC
User EXEC

IP address The IP address of the client.

Hardware Address The MAC address or the client identifier.

Lease expiration The lease expiration time of the IP address assigned to the client.

Type The manner in which IP address was assigned to the client.

4.8.25 show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format `show ip dhcp global configuration`

Modes Privileged EXEC
User EXEC

Service DHCP The field to display the status of dhcp protocol.

Number of Ping Packets The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.

Conflict Logging Shows whether conflict logging is enabled or disabled.

BootP Automatic Shows whether BootP for dynamic pools is enabled or disabled.

4.8.26 show ip dhcp pool configuration

This command displays pool configuration. If `all` is specified, configuration for all the pools is displayed.

Format `show ip dhcp pool configuration` *{<name> | all}*

Modes Privileged EXEC
User EXEC

Pool Name The name of the configured pool.

Pool Type The pool type.

Lease Time The lease expiration time of the IP address assigned to the client.

DNS Servers The list of DNS servers available to the DHCP client

Default Routers The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

Network The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Client Name The name of a DHCP client.

Client Identifier The unique identifier of a DHCP client.

Hardware Address The hardware address of a DHCP client.

Hardware Address Type The protocol of the hardware platform.

Host The IP address and the mask for a manual binding to a DHCP client.

4.8.27 show ip dhcp server statistics

This command displays DHCP server statistics.

Format `show ip dhcp server statistics`

Modes Privileged EXEC
User EXEC

Automatic Bindings The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.

Expired Bindings The number of expired leases.

Malformed Bindings The number of truncated or corrupted messages that were received by the DHCP server.

Message Received:

DHCP DISCOVER The number of DHCPDISCOVER messages the server has received.

DHCP REQUEST The number of DHCPREQUEST messages the server has received.

DHCP DECLINE The number of DHCPDECLINE messages the server has received.

DHCP RELEASE The number of DHCPRELEASE messages the server has received.

DHCP INFORM The number of DHCPINFORM messages the server has received.

Message Sent:

DHCP OFFER The number of DHCPOFFER messages the server sent.

DHCP ACK The number of DHCPACK messages the server sent.

DHCP NACK The number of DHCPNACK messages the server sent.

4.8.28 show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Format `show ip dhcp conflict` *[<ip-address>]*

Modes Privileged EXEC
User EXEC

IP address The IP address of the host as recorded on the DHCP server.

Detection Method The manner in which the IP address of the hosts were found on the DHCP Server

Detection time The time when the conflict was found.

4.9 DHCP Filtering

You can configure the DHCP Filtering feature as a security measure against unauthorized DHCP servers. DHCP filtering works by allowing you to configure each port as either a trusted port or an untrusted port. To optimize the DHCP filtering feature, configure the port that is connected to an authorized DHCP server on your network as a trusted port. Any DHCP responses received on a trusted port are forwarded. Make sure that all other ports are untrusted so that any DHCP (or BootP) responses received are discarded.

You can configure DHCP filtering on physical ports and LAGs. DHCP filtering is not operable on VLAN interfaces.

4.9.1 ip dhcp filtering

This command enables DHCP filtering globally.

Default disabled

Format `ip dhcp filtering`

Mode Global Config

4.9.1.1 no ip dhcp filtering

This command disables DHCP filtering.

Format `no ip dhcp filtering`

Mode Global Config

4.9.2 ip dhcp filtering trust

This command configures an interface as trusted.

Default untrusted

Format `ip dhcp filtering trust`

Mode Interface Config

4.9.2.1 no ip dhcp filtering trust

This command returns an interface to the default value for DHCP filtering.

Format `no ip dhcp filtering trust`

Mode Interface Config

4.9.3 show ip dhcp filtering

This command displays the DHCP filtering configuration.

Format `show ip dhcp filtering`

Mode Privileged EXEC

Interface The interface by slot/port.

Trusted Indicates whether the interface is trusted or untrusted.

4.10 Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their FASTPATH product.

CAUTION: The output of "debug" commands can be long and may adversely affect system performance.

4.10.1 debug console

This command enables the display of "debug" trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default disabled

Format `debug console`

Mode Privileged EXEC

4.10.1.1 no debug console

This command disables the display of "debug" trace output on the login session in which it is executed.

Format `no debug console`

Mode Privileged EXEC

4.10.2 debug clear

This command disables all previously enabled "debug" traces.

Default none

Format `debug clear`

Mode Privileged EXEC

4.10.3 debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default disabled

Format `debug spanning-tree bpdu transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]:
dot1s_debug.c(1249) 101 % Pkt TX - Intf: 1/0/7(7), Source_Mac:
00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00,
Root_Priority: 0x8000 Path_Cost: 0
```

The following parameters are displayed in the trace message:

TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is port/slot (internal interface number).
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

4.10.3.1 no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format `no debug spanning-tree bpdu transmit`

Mode Privileged EXEC

4.10.4 debug spanning-tree bpdu receive

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default disabled

Format `debug spanning-tree bpdu receive`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]:
dot1s_debug.c(1249) 101 % Pkt RX - Intf: 1/0/9(9), Source_Mac:
00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root
Priority: 0x8000 Path Cost: 0
```

The following parameters are displayed in the trace message:

RX	A packet received by the device.
Intf	The interface that the packet came in on. Format used is port/slot (internal interface number).
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

4.10.4.1 no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format `no debug spanning-tree bpdu receive`

Mode Privileged EXEC

4.10.5 debug spanning-tree bpdu

This command enables tracing of spanning tree bpdus received and transmitted by the switch.

Default disabled

Format `debug spanning-tree bpdu`

Mode Privileged EXEC

4.10.5.1 no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format `no debug spanning-tree bpdu`

Mode Privileged EXEC

4.10.6 debug igmpsnooping packet transmit

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default disabled

Format `debug igmpsnooping packet transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]:
igmp_snooping_debug.c(116) 908 % Pkt TX - Intf: 1/0/20(20), Vlan_Id:1
Src_Mac: 00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01 Src_IP: 9.1.1.1
Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group: 225.0.0.1
```

The following parameters are displayed in the trace message:

TX A packet transmitted by the device.

Intf The interface that the packet went out on. Format used is slot/port (internal interface number).

Src_Mac Source MAC address of the packet.

Dest_Mac Destination multicast MAC address of the packet.

Src_IP The source IP address in the IP header in the packet.

Dest_IP The destination multicast IP address in the packet.

Type The type of IGMP packet. Type can be one of the following:
Membership Query – IGMP Membership Query
V1_Membership_Report – IGMP Version 1 Membership Report

V2_Membership_Report – IGMP Version 2 Membership Report
V3_Membership_Report – IGMP Version 3 Membership Report
V2_Leave_Group – IGMP Version 2 Leave Group

Group Multicast group address in the IGMP header.

4.10.6.1 no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format `no debug igmpsnooping transmit`

Mode Privileged EXEC

4.10.7 debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default disabled

Format `debug igmpsnooping packet receive`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]:
igmp_snooping_debug.c(116) 908 % Pkt RX - Intf: 1/0/20(20), Vlan_Id:1
Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05 Src_IP: 11.1.1.1
Dest_IP: 225.0.0.5 Type: Membership_Query Group: 225.0.0.5
```

The following parameters are displayed in the trace message:

RX A packet received by the device.

Intf The interface that the packet went out on. Format used is slot/port (internal interface number).

Src_Mac Source MAC address of the packet.

Dest_Mac Destination multicast MAC address of the packet.

Src_IP The source IP address in the ip header in the packet.

Dest_IP The destination multicast ip address in the packet.

Type The type of IGMP packet. Type can be one of the following:
Membership_Query – IGMP Membership Query
V1_Membership_Report – IGMP Version 1 Membership Report
V2_Membership_Report – IGMP Version 2 Membership Report
V3_Membership_Report – IGMP Version 3 Membership Report
V2_Leave_Group – IGMP Version 2 Leave Group

Group Multicast group address in the IGMP header.

4.10.7.1 no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format `no debug igmpsnooping receive`

Mode Privileged EXEC

4.10.8 debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default disabled

Format `debug igmpsnooping packet`

Mode Privileged EXEC

4.10.8.1 no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format `no debug igmpsnooping packet`

Mode Privileged EXEC

4.10.9 debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/ serviceport for switching packages. For routing packages, pings are traced on the routing ports as well.

Default disabled

Format `debug ping packet`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128)
20 % Pkt TX - Intf: 1/0/1(1),
SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST

<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21
% Pkt RX - Intf: 1/0/1(1), S
RC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

TX/RX TX refers to a packet transmitted by the device. RX refers to packets received by the device.

Intf The interface that the packet came in or went out on. Format used is slot/port (internal interface number).

SRC_IP The source IP address in the IP header in the packet.

DEST_IP The destination IP address in the IP header in the packet.

Type Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

4.10.9.1 no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format `no debug ping packet`

Mode Privileged EXEC

4.10.10 debug rip packet

This command turns on tracing of RIP requests and responses. This command takes no options. The output is directed to the log file.

Default disabled

Format `debug rip packet`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:35:15 192.168.17.29-1 RIP[181783160]:
rip_map_debug.c(96) 775 %
Pkt RX on Intf: 1/0/1(1), Src_IP:43.1.1.1 Dest_IP:43.1.1.2
Rip_Version: RIPv2 Packet_Type:RIP_RESPONSE
ROUTE 1): Network: 10.1.1.0 Mask: 255.255.255.0 Metric: 1
ROUTE 2): Network: 40.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 3): Network: 10.50.50.0 Mask: 255.255.255.0 Metric: 1
ROUTE 4): Network: 41.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 5): Network:42.0.0.0 Mask:255.0.0.0 Metric:1
Another 6 routes present in packet not displayed.
```

The following parameters are displayed in the trace message:

TX/RX TX refers to a packet transmitted by the device. RX refers to packets received by the device.

Intf The interface that the packet came in or went out on. Format used is slot/port (internal interface number).

Src_IP The source IP address in the IP header of the packet.

Dest_IP The destination IP address in the IP header of the packet.

Rip_Version RIP version used <RIPv1 or RIPv2>.

Packet_Type Type of RIP packet. <RIP_REQUEST or RIP_RESPONSE>.

Routes Up to 5 routes in the packet are displayed in the following format:
Network: <a.b.c.d> Mask <a.b.c.d> Next_Hop <a.b.c.d> Metric <a>
The next hop is only displayed if it is different from 0.0.0.0.
For RIPv1 packets, Mask is always 0.0.0.0.

Number of routes not printed Only the first five routes present in the packet are included in the trace. There is another notification of the number of additional routes present in the packet that were not included in the trace.

4.10.10.1 no debug rip packet

This command disables tracing of RIP requests and responses.

Format `no debug rip packet`

Mode Privileged EXEC

4.10.11 debug ospf packet

This command enables tracing of OSPF packets received and transmitted by the switch.

Default disabled

Format `debug ospf packet`

Mode Privileged EXEC

Sample outputs of the trace messages are shown below.

```
<15> JAN 02 11:03:31 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297)
25430 % Pkt RX - Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:224.0.0.5 AreaId:0.0.0.0 Type:HELLO
NetMask:255.255.255.0 D
esigRouter:0.0.0.0 Backup:0.0.0.0

<15> JAN 02 11:03:35 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293)
25431 % Pkt TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:DB_DSCR Mtu:1500
Options:E
Flags: I/M/MS Seq:126166

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297)
25434 % Pkt RX - Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:192.168.50.1 AreaId:0.0.0.0 Type:LS_REQ Length:
1500

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293)
25435 % Pkt TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:LS_UPD Length:
1500
```

The following parameters are displayed in the trace message:

TX/RX TX refers to a packet transmitted by the device. RX refers to packets received by the device.

Intf The interface that the packet came in or went out on. Format used is slot/port (internal interface number).

SrcIp The source IP address in the IP header of the packet.

DestIp The destination IP address in the IP header of the packet.

AreaId The area ID in the OSPF header of the packet.

Type Could be one of the following:
HELLO – Hello packet
DB_DSCR – Database descriptor
LS_REQ – LS Request
LS_UPD – LS Update
LS_ACK – LS Acknowledge

The remaining fields in the trace are specific to the type of OSPF Packet.

HELLO packet field definitions:

Netmask The netmask in the hello packet.

DesignRouter Designated Router IP address.

Backup Backup router IP address.

DB_DSCR packet field definitions:

MTU MTU

Options Options in the OSPF packet.

Flags Could be one or more of the following:
I – Init
M – More
MS – Master/Slave

Seq Sequence Number of the DD packet.

LS_REQ packet field definitions:

Length Length of packet.

LS_UPD packet field definitions.

Length Length of packet.

LS_ACK packet field definitions.

Length Length of packet.

4.10.11.1 no debug ospf packet

This command disables tracing of OSPF packets.

Format `no debug ospf packet`

Mode Privileged EXEC

4.10.12 debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default disabled

Format `debug lacp packet`

Mode Privileged

A sample output of the trace message is shown below.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]:
dot3ad_debug.c(385) 58 %% Pkt TX - Intf: 1/0/1(1), Type: LACP, Sys:
00:11:88:14:62:e1, State: 0x47, Key: 0x36
```

4.10.12.1 no debug lacp packet

This command disables tracing of LACP packets.

Format `no debug lacp packet`

Mode Privileged EXEC

Chapter 5

Management Commands

5. Management Commands

This chapter describes the management commands available in the CLI.

The Management Commands chapter contains the following sections:

- 5.1 “Network Interface Commands” on page 5 - 2
- 5.2 “Console Port Access Commands” on page 5 - 5
- 5.3 “Telnet Commands” on page 5 - 6
- 5.4 “Secure Shell (SSH) Command” on page 5 - 10
- 5.5 “User Account Commands” on page 5 - 12
- 5.6 “SNMP Commands” on page 5 - 15
- 5.7 “CLI Command Logging Command” on page 5 - 23
- 5.8 “RADIUS Commands” on page 5 - 23
- 5.9 “TACACS+ Commands” on page 5 - 29
- 5.10 “Configuration Scripting Commands” on page 5 - 31
- 5.11 “Pre-login Banner and System Prompt Commands” on page 5 - 33
- 5.12 “Watchdog Support Commands” on page 5 - 33
- 5.13 “Diagnostics Commands” on page 5 - 34
- 5.14 “PCI express Commands” on page 5 - 34
- 5.15 “Storage Commands” on page 5 - 36
- 5.16 “Clock Support Commands” on page 5 - 37

The commands in this chapter are divided into three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.

5.1 Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see 2.3.2 “network mgmt_vlan” on page 2 - 18

5.1.1 enable (Privileged EXEC access)

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

Format `enable`

Mode User EXEC

5.1.2 serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port.

Format `serviceport ip` *<ipaddr> <netmask> [gateway]*

Mode Privileged EXEC

5.1.3 serviceport protocol

This command specifies the network management port configuration protocol. If you modify this value, the change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Format `serviceport protocol` *{none | bootp | dhcp}*

Mode Privileged EXEC

5.1.4 network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet.

Format `network parms` *<ipaddr> <netmask> [<gateway>]*

Mode Privileged EXEC

5.1.5 network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Default none

Format `network protocol` *{none | bootp | dhcp}*

Mode Privileged EXEC

5.1.6 network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format `network mac-address` *<macaddr>*

Mode Privileged EXEC

5.1.7 network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

Default burnedin

Format `network mac-type` *{local | burnedin}*

Mode Privileged EXEC

5.1.7.1 no network mac-type

This command resets the value of MAC address to its default.

Format `no network mac-type`

Mode Privileged EXEC

5.1.8 show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

Format `show network`

Modes Privileged EXEC
User EXEC

IP Address The IP address of the interface. The factory default value is 0.0.0.0

Subnet Mask The IP subnet mask for this interface. The factory default value is 0.0.0.0

Default Gateway The default gateway for this IP interface. The factory default value is 0.0.0.0

Burned In MAC Address The burned in MAC address used for in-band connectivity.

Locally Administered MAC Address If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.

MAC Address Type The MAC address should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.

Network Configuration Protocol Current The network protocol is being used. The options are bootp | dhcp | none.

5.1.9 show serviceport

This command displays service port configuration information.

Format `show serviceport`

Mode Privileged EXEC

IP Address The IP address of the interface. The factory default value is 0.0.0.0

Subnet Mask The IP subnet mask for this interface. The factory default value is 0.0.0.0

Default Gateway The default gateway for this IP interface. The factory default value is 0.0.0.0

ServPort Configuration Protocol Current The network protocol used on the last, or current power-up cycle, if any.

Burned in MAC Address The burned in MAC address used for in-band connectivity.

5.2 Console Port Access Commands

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

5.2.1 configuration

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

Format `configuration`

Mode Privileged EXEC

5.2.2 lineconfig

This command gives you access to the Line Config mode, which allows you to configure various Telnet settings and the console port.

Format `lineconfig`

Mode Global Config

5.2.3 serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default 9600

Format `serial baudrate` *{1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}*

Mode Line Config

5.2.3.1 no serial baudrate

This command sets the communication rate of the terminal interface.

Format `no serial baudrate`

Mode Line Config

5.2.4 serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default 5

Format `serial timeout` *<0-160>*

Mode Line Config

5.2.4.1 no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

Format `no serial timeout`

Mode Line Config

5.2.5 show serial

This command displays serial communication settings for the switch.

Format `show serial`

Modes Privileged EXEC
User EXEC

Serial Port Login Timeout (minutes) The time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.

Baud Rate (bps) The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud. The factory default is 9600 baud.

Character Size (bits) The number of bits in a character. The number of bits is always 8.

Flow Control Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.

Stop Bits The number of Stop bits per character. The number of Stop bits is always 1.

Parity Type The Parity Method used on the Serial Port. The Parity Method is always None.

5.3 Telnet Commands

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

5.3.1 ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default enabled

Format `ip telnet server enable`

Mode Privileged EXEC

5.3.1.1 no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format `no ip telnet server enable`

Mode Privileged EXEC

5.3.2 telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If *[debug]* is used, the current Telnet options enabled is displayed. The optional *line* parameter sets the outbound Telnet operational mode as 'linemode', where by default, the operational mode is 'character mode'. The *noecho* option disables local echo.

Format `telnet` *<host> <port> [debug] [line] [noecho]*

Modes Privileged EXEC
User EXEC

5.3.3 transport input telnet

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.

NOTE: If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the `ip telnet server enable` command to enable Telnet Server Admin Mode.

Default enabled

Format `transport input telnet`

Mode Line Config

5.3.3.1 no transport input telnet

Use this command to prevent new Telnet sessions from being established.

Format `no transport input telnet`

Mode Line Config

5.3.4 transport output telnet

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

Default enabled

Format `transport output telnet`

Mode Line Config

5.3.4.1 no transport output telnet

Use this command to prevent new outbound Telnet connection from being established.

Format `no transport output telnet`

Mode Line Config

5.3.5 session-limit

This command specifies the maximum number of simultaneous outbound Telnet sessions. A value of 0 indicates that no outbound Telnet session can be established.

Default 5

Format `session-limit` *<0-5>*

Mode Line Config

5.3.5.1 no session-limit

This command sets the maximum number of simultaneous outbound Telnet sessions to the default value.

Format `no session-limit`

Mode Line Config

5.3.6 session-timeout

This command sets the Telnet session timeout value.The timeout value unit of time is minutes. A value of 0 indicates that a session remains active indefinitely.

Default 0

Format `session-timeout` *<0-160>*

Mode Line Config

5.3.6.1 no session-timeout

This command sets the Telnet session timeout value to the default. The timeout value unit of time is minutes.

Format `no session-timeout`

Mode Line Config

5.3.7 telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

Default 5

Format `telnetcon maxsessions` *<0-5>*

Mode Privileged EXEC

5.3.7.1 no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

Format `no telnetcon maxsessions`

Mode Privileged EXEC

5.3.8 telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

NOTE: When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Default 5

Format `telnetcon timeout` *<1-160>*

Mode Privileged EXEC

5.3.8.1 no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.

NOTE: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration.

Format `no telnetcon timeout`

Mode Privileged EXEC

5.3.9 disconnect

Use the `disconnect` command to close Telnet or SSH sessions. Use *all* to close all Telnet and SSH sessions, or use <*session-id*> to specify the session ID to close. To view the possible values for <*session-id*>, use the `show loginsession` command.

Format `disconnect` *{<session_id> | all}*

Mode Privileged EXEC

5.3.10 show loginsession

This command displays current Telnet and serial port connections to the switch.

Format `show loginsession`

Mode Privileged EXEC

ID Login Session ID

User Name The name the user will use to login using the serial port or Telnet.

Connection From IP address of the Telnet client machine or EIA-232 for the serial port connection.

Idle Time Time this session has been idle.

Session Time Total time this session has been connected.

5.3.11 show telnet

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system.

Format `show telnet`

Modes Privileged EXEC
User EXEC

Outbound Telnet Login Timeout The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.

Maximum Number of Outbound Telnet Sessions The number of simultaneous outbound Telnet connections allowed.

Allow New Outbound Telnet Sessions Indicates whether outbound Telnet sessions will be allowed.

5.3.12 show telnetcon

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format `show telnetcon`

Modes Privileged EXEC
User EXEC

Remote Connection Login Timeout (minutes) This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.

Maximum Number of Remote Connection Sessions This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.

Allow New Telnet Sessions New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

5.4 Secure Shell (SSH) Command

This section describes the commands you use to configure SSH access to the switch. Use SSH to access the switch from a remote management host.

NOTE: The system allows a maximum of 5 SSH sessions.

5.4.1 ip ssh

Use this command to enable SSH access to the system.

Default disabled

Format `ip ssh`

Mode Privileged EXEC

5.4.1.1 no ip ssh

Use this command to disable SSH access to the system.

Format `no ip ssh`

Mode Privileged EXEC

5.4.2 ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default 1 and 2

Format `ip ssh protocol` *[1] [2]*

Mode Privileged EXEC

5.4.3 ip ssh server enable

This command enables the IP secure shell server.

Default disabled

Format `ip ssh server enable`

Mode Privileged EXEC

5.4.3.1 no ip ssh server enable

This command disables the IP secure shell server.

Format `no ip ssh server enable`

Mode Privileged EXEC

5.4.4 sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

Default 5

Format `sshcon maxsessions` *<0-5>*

Mode Privileged EXEC

5.4.4.1 no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

Format `no sshcon maxsessions`

Mode Privileged EXEC

5.4.5 sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Default 5

Format `sshcon timeout` *<1-160>*

Mode Privileged EXEC

5.4.5.1 no sshcon timeout

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Format `no sshcon timeout`

Mode Privileged EXEC

5.4.6 show ip ssh

This command displays the ssh settings.

Format `show ip ssh`

Mode Privileged EXEC

Administrative Mode This field indicates whether the administrative mode of SSH is enabled or disabled.

Protocol Level The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.

Connections This field specifies the current SSH connections.

5.5 User Account Commands

This section describes the commands you use to add, manage, and delete system users. FASTPATH software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

NOTE: You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

5.5.1 users name

This command adds a new user account, if space permits. The account *<username>* can be up to eight characters in length. You can use alphanumeric characters as well as the dash (‘-’) and underscore (‘_’). You can define up to six user names.

NOTE: The <*username*> is not case sensitive when you add and delete users, and when the user logs in. However, when you use the <*username*> to set the user password, authentication, or encryption, you must enter the <*username*> in the same case you used when you added the user. To see the case of the <*username*>, enter the **`show users`** command.

Format **`users name`** <*username*>

Mode Global Config

5.5.1.1 no users name

This command removes a user account.

Format **`no users name`** <*username*>

Mode Global Config

NOTE: You cannot delete the “admin” user account.

5.5.2 users passwd

Use this command to change a password. Passwords are a maximum of eight alphanumeric characters. If a user is authorized for authentication or encryption is enabled, the password length must be at least eight alphanumeric characters. The password is case sensitive. When you change a password, a prompt asks for the old password. If there is no password, press enter. You must enter the <*username*> in the same case you used when you added the user. To see the case of the <*username*>, enter the **`show users`** command.

NOTE: To specify a blank password in the configuration script, you must specify it as a space within quotes, for example, “ ”. For more information about creating configuration scripts, see 5.10 “Configuration Scripting Commands” on page 5 - 31.

Default no password

Format **`users passwd`** <*username*>

Mode Global Config

5.5.2.1 no users passwd

This command sets the password of an existing user to blank. When you change a password, a prompt asks for the old password. If there is no password, press enter.

Format **`no users passwd`** <*username*>

Mode Global Config

5.5.3 users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are **`readonly`** or **`readwrite`**. The <*username*> is the login user name for which the specified access mode applies. The default is **`readwrite`** for the “admin” user and **`readonly`** for all other users. You must enter the <*username*> in the same case you used when you added the user. To see the case of the <*username*>, enter the **`show users`** command.

Default admin - readwrite
other - readonly

Format **`users snmpv3 accessmode`** <*username*> *{readonly | readwrite}*

Mode Global Config

5.5.3.1 no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified user as **readwrite** for the "admin" user and **readonly** for all other users. The <*username*> value is the user name for which the specified access mode will apply.

Format **`no users snmpv3 accessmode`** <*username*>

Mode Global Config

5.5.4 users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are **`none`**, **`md5`** or **`sha`**. If you specify **`md5`** or **`sha`**, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The <*username*> is the user name associated with the authentication protocol. You must enter the <*username*> in the same case you used when you added the user. To see the case of the <*username*>, enter the **`show users`** command.

Default no authentication

Format **`users snmpv3 authentication`** <*username*> *{none | md5 | sha}*

Mode Global Config

5.5.4.1 no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified user to **none**. The <*username*> is the user name for which the specified authentication protocol is used.

Format **`no users snmpv3 authentication`** <*username*>

Mode Global Config

5.5.5 users snmpv3 encryption

This command specifies the encryption protocol used for the specified user. The valid encryption protocols are **`des`** or **`none.`**

If you select **`des`**, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the **`des`** protocol but do not provide a key, the user is prompted for the key. When you use the **`des`** protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select **`none`**, you do not need to provide a key.

The <*username*> value is the login user name associated with the specified encryption. You must enter the <*username*> in the same case you used when you added the user. To see the case of the <*username*>, enter the **`show users`** command.

Default no encryption

Format `users snmpv3 encryption` *<username> {none | des[key]}*

Mode Global Config

5.5.5.1 no users snmpv3 encryption

This command sets the encryption protocol to **none**. The *<username>* is the login user name for which the specified encryption protocol will be used.

Format `no users snmpv3 encryption` *<username>*

Mode Global Config

5.5.6 show users

This command displays the configured user names and their settings. This command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format `show users`

Mode Privileged EXEC

User Name The name the user enters to login using the serial port, Telnet or Web.

Access Mode Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the "admin" user has Read/Write access and the "guest" has Read Only access. There can only be one Read/Write user and up to five Read Only users.

SNMPv3 Access Mode The SNMPv3 Access Mode. If the value is set to `ReadWrite`, the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to `ReadOnly`, the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.

SNMPv3 Authentication The authentication protocol to be used for the specified login user.

SNMPv3 Encryption The encryption protocol to be used for the specified login user.

5.6 SNMP Commands

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

5.6.1 snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for *<name>*, *<loc>* and *<con>* is from 1 to 31 alphanumeric characters.

Default none

Format `snmp-server` *{sysname <name> | location <loc> | contact <con>}*

Mode Global Config

5.6.2 snmp-server community

This command adds (and names) a new SNMP community. A community <*name*> is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of <*name*> can be up to 16 case-sensitive characters.

NOTE: Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default public and private, which you can rename
default values for the remaining four community names are blank

Format `snmp-server community` <*name*>

Mode Global Config

5.6.2.1 no snmp-server community

This command removes this community name from the table. The <*name*> is the community name to be deleted.

Format `no snmp-server community` <*name*>

Mode Global Config

5.6.3 snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Default 0.0.0.0

Format `snmp-server community ipaddr` <*ipaddr*> <*name*>

Mode Global Config

5.6.3.1 no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

Format `no snmp-server community ipaddr` <*name*>

Mode Global Config

5.6.4 snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Default 0.0.0.0

Format **snmp-server community ipmask** <*ipmask*> <*name*>

Mode Global Config

5.6.4.1 no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

Format **no snmp-server community ipmask** <*name*>

Mode Global Config

5.6.5 snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Default private and public communities - enabled
other four - disabled

Format **snmp-server community mode** <*name*>

Mode Global Config

5.6.5.1 no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Format **no snmp-server community mode** <*name*>

Mode Global Config

5.6.6 snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Format **snmp-server community ro** <*name*>

Mode Global Config

5.6.7 snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format **snmp-server community rw** <*name*>

Mode Global Config

5.6.8 snmp-server enable traps violation

This command enables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

NOTE: For other port security commands, see 2.6 “Protected Ports Commands” on page 2 - 30.

Default disabled

Format `snmp-server enable traps violation`

Mode Interface Config

5.6.8.1 no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format `no snmp-server enable traps violation`

Mode Interface Config

5.6.9 snmp-server enable traps

This command enables the Authentication Flag.

Default enabled

Format `snmp-server enable traps`

Mode Global Config

5.6.9.1 no snmp-server enable traps

This command disables the Authentication Flag.

Format `no snmp-server enable traps`

Mode Global Config

5.6.10 snmp-server enable traps bcaststorm

This command enables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

Default enabled

Format `snmp-server enable traps bcaststorm`

Mode Global Config

5.6.10.1 no snmp-server enable traps bcaststorm

This command disables the broadcast storm trap. When enabled, broadcast storm traps are sent only if the broadcast storm recovery mode setting associated with the port is enabled.

Format `no snmp-server enable traps bcaststorm`

Mode Global Config

5.6.11 snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See “snmp trap link-status” on page 5 - 21.

Default enabled

Format `snmp-server enable traps linkmode`

Mode Global Config

5.6.11.1 no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format `no snmp-server enable traps linkmode`

Mode Global Config

5.6.12 snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default enabled

Format `snmp-server enable traps multiusers`

Mode Global Config

5.6.12.1 no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format `no snmp-server enable traps multiusers`

Mode Global Config

5.6.13 snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default enabled

Format `snmp-server enable traps stpmode`

Mode Global Config

5.6.13.1 no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

Format `no snmp-server enable traps stpmode`

Mode Global Config

5.6.14 snmptrap

This command adds an SNMP trap receiver. The maximum length of <*name*> is 16 case-sensitive alphanumeric characters. The <*snmpversion*> is the version of SNMP. The version parameter options are snmpv1 or snmpv2.

NOTE: The <*name*> parameter does not need to be unique, however; the <*name*> and <*ipaddr*> pair must be unique. Multiple entries can exist with the same <*name*>, as long as they are associated with a different <*ipaddr*>. The reverse scenario is also acceptable. The <*name*> is the community name used when sending the trap to the receiver, but the <*name*> is not directly associated with the SNMP Community Table, See "snmp-server community" on page39."

Default snmpv2

Format **`snmptrap`** <*name*> <*ipaddr*> *[snmpversion <snmpversion>]*

Mode Global Config

5.6.14.1 no snmptrap

This command deletes trap receivers for a community.

Format **`no snmptrap`** <*name*> <*ipaddr*>

Mode Global Config

5.6.15 snmptrap snmpversion

This command modifies the SNMP version of a trap. The maximum length of <*name*> is 16 case-sensitive alphanumeric characters. The <*snmpversion*> parameter options are snmpv1 or snmpv2.

NOTE: This command does not support a "no" form.

Default snmpv2

Format **`snmptrap snmpversion`** <*name*> <*ipaddr*> <*snmpversion*>

Mode Global Config

5.6.16 snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

NOTE: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Format **`snmptrap ipaddr`** <*name*> <*ipaddrold*> <*ipaddrnew*>

Mode Global Config

5.6.17 snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Format `snmptrap mode` <*name*> <*ipaddr*>

Mode Global Config

5.6.17.1 no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are unable to receive traps.

Format `no snmptrap mode` <*name*> <*ipaddr*>

Mode Global Config

5.6.18 snmp trap link-status

This command enables link status traps by interface.

NOTE: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 5 - 19.

Format `snmp trap link-status`

Mode Interface Config

5.6.18.1 no snmp trap link-status

This command disables link status traps by interface.

NOTE: This command is valid only when the Link Up/Down Flag is enabled.

Format `no snmp trap link-status`

Mode Interface Config

5.6.19 snmp trap link-status all

This command enables link status traps for all interfaces.

NOTE: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 5 - 19.

Format `snmp trap link-status all`

Mode Global Config

5.6.19.1 no snmp trap link-status all

This command disables link status traps for all interfaces.

NOTE: This command is valid only when the Link Up/Down Flag is enabled. See “snmp-server enable traps linkmode” on page 5 - 19.

Format `no snmp trap link-status all`

Mode Global Config

5.6.20 show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Versions 1, 2 or 3. For more information about the SNMP specification, see the SNMP RFCs. The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format `show snmpcommunity`

Mode Privileged EXEC

SNMP Community Name The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.

Client IP Address An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP address. Note: If the Subnet Mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0

Client IP Mask A mask to be ANDed with the requesting entity's IP address before comparison with IP address. If the result matches with IP address then the address is an authenticated IP address. For example, if the IP address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0

Access Mode The access level for this community string.

Status The status of this community access entry.

5.6.21 show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format `show snmptrap`

Mode Privileged EXEC

SNMP Trap Name The community string of the SNMP trap packet sent to the trap manager. The string is case sensitive and can be up to 16 alphanumeric characters.

IP Address The IP address to receive SNMP traps from this device.

Status The receiver's status (enabled or disabled).

5.6.22 show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`

Mode Privileged EXEC

Authentication Flag Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.

Link Up/Down Flag Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.

Multiple Users Flag Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).

Spanning Tree Flag Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.

ACL Traps May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.

DVMRP Traps Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.

OSPF Traps Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent.

PIM Traps Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.

5.7 CLI Command Logging Command

This section describes the commands you use to configure CLI Command Logging.

5.7.1 logging cli-command

This command enables the CLI command logging feature, which enables the FASTPATH software to log all CLI commands issued on the system.

Default enabled

Format `logging cli-command`

Mode Global Config

5.7.1.1 no logging cli-command

This command disables the CLI command Logging feature.

Format `no logging cli-command`

Mode Global Config

5.8 RADIUS Commands

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

5.8.1 radius accounting mode

This command is used to enable the RADIUS accounting function.

Default disabled

Format `radius accounting mode`

Mode Global Config

5.8.1.1 no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format `no radius accounting mode`

Mode Global Config

5.8.2 radius server host

This command is used to configure the RADIUS authentication and accounting server. If you use the <*auth*> parameter, the command configures the IP address to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the “no” form of the command. If you use the optional <*port*> parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The <*port*> number range is 1 - 65535, with 1812 being the default value.

NOTE: To re-configure a RADIUS authentication server to use the default UDP <*port*>, set the <*port*> parameter to 1812.

If you use the <*acct*> token, the command configures the IP address to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the “no” form of the command to remove it from the configuration. The IP address you specify must match that of a previously configured accounting server. If you use the optional <*port*> parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a <*port*> is already configured for the accounting server, the new <*port*> replaces the previously configured <*port*>. The <*port*> must be a value in the range 1 - 65535, with 1813 being the default.

NOTE: To re-configure a RADIUS accounting server to use the default UDP <*port*>, set the <*port*> parameter to 1813.

Format `radius server host` *{auth | acct} <ipaddr> [<port>]*

Mode Global Config

5.8.2.1 no radius server host

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The <*ipaddr*> parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

Format `no radius server host` *{auth | acct} <ipaddress>*

Mode Global Config

5.8.3 radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the 'auth' or 'acct' token is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret is prompted.

NOTE: The secret must be an alphanumeric value not exceeding 16 characters.

Format `radius server key` *{auth | acct} <ipaddr>*

Mode Global Config

5.8.4 radius server msgauth

This command enables the message authenticator attribute for a specified server.

Format `radius server msgauth` *<ipaddr>*

Mode Global Config

5.8.4.1 no radius server msgauth

This command disables the message authenticator attribute for a specified server.

Format `no radius server msgauth` *<ipaddr>*

Mode Global Config

5.8.5 radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server handles RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. You can configure up to three servers on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Format `radius server primary` *<ipaddr>*

Mode Global Config

5.8.6 radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

Default 4

Format `radius server retransmit` *<retries>*

Mode Global Config

5.8.6.1 no radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted, to the default value.

Format `no radius server retransmit`

Mode Global Config

5.8.7 radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default 5

Format `radius server timeout` <*seconds*>

Mode Global Config

5.8.7.1 no radius server timeout

This command sets the timeout value to the default value.

Format `no radius server timeout`

Mode Global Config

5.8.8 show radius

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items are displayed.

Format `show radius` *[servers]*

Mode Privileged EXEC

Primary Server IP Address The configured server currently in use for authentication.

Number of configured servers The configured IP address of the authentication server.

Max number of retransmits The configured value of the maximum number of times a request packet is retransmitted.

Timeout Duration The configured timeout value, in seconds, for request re-transmissions.

Accounting Mode Yes or No.

If you use the *[servers]* keyword, the following information displays:

IP Address IP address of the configured RADIUS server.

Port The port in use by this server.

Type Primary or secondary.

Secret Configured Yes / No.

Message Authenticator The message authenticator attribute for the selected server, which can be enables or disables.

5.8.9 show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

Format `show radius accounting` *[statistics <ipaddr>]*

Mode Privileged EXEC

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Mode Enabled or disabled

IP Address The configured IP address of the RADIUS accounting server.

Port The port in use by the RADIUS accounting server.

Secret Configured Yes or No.

If you use the optional *statistics <ipaddr>* parameter, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Accounting Server IP Address IP address of the configured RADIUS accounting server

Round Trip Time The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.

Requests The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.

Retransmission The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.

Responses The number of RADIUS packets received on the accounting port from this server.

Malformed Responses The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.

Bad Authenticators The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.

Pending Requests The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.

Timeouts The number of accounting timeouts to this server.

Unknown Types The number of RADIUS packets of unknown types, which were received from this server on the accounting port.

Packets Dropped The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

5.8.10 show radius statistics

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Format `show radius statistics` *[<ipaddr>]*

Mode Privileged EXEC

If you do not specify the IP address, then only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

Invalid Server Addresses The number of RADIUS Access-Response packets received from unknown addresses.

Server IP Address IP address of the Server.

Round Trip Time The time interval, in hundredths of a second, between the most recent Access-Reply, Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.

Access Requests The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.

Access Retransmission The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

Access Accepts The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.

Access Rejects The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.

Access Challenges The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.

Malformed Access Responses The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.

Bad Authenticators The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.

Pending Requests The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.

Timeouts The number of authentication timeouts to this server.

Unknown Types The number of RADIUS packets of unknown types, which were received from this server on the authentication port.

Packets Dropped The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

5.9 TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

5.9.1 tacacs-server host

Use the **`tacacs-server host`** command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The <*ip-address*> parameter is the IP address of the TACACS+ server. To specify multiple hosts, multiple **`tacacs-server host`** commands can be used.

Format **`tacacs-server host`** <*ip-address*>

Mode Global Config

5.9.1.1 no tacacs-server host

Use the **`no tacacs-server host`** command to delete the specified hostname or IP address. The <*ip-address*> parameter is the IP address of the TACACS+ server.

Format **`no tacacs-server host`** <*ip-address*>

Mode Global Config

5.9.2 tacacs-server key

Use the **`tacacs-server key`** command to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The <*key-string*> parameter has a range of 0 - 128 characters and specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon.

Format **`tacacs-server key`** <*key-string*>

Mode Global Config

5.9.2.1 no tacacs-server key

Use the **`no tacacs-server key`** command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The <*key-string*> parameter has a range of 0 - 128 characters This key must match the key used on the TACACS+ daemon.

Format **`no tacacs-server key`** <*key-string*>

Mode Global Config

5.9.3 tacacs-server timeout

Use the **tacacs-server timeout** command to set the timeout value for communication with the TACACS+ servers. The <*timeout*> parameter has a range of 1-30 and is the timeout value in seconds.

Default 5

Format **tacacs-server timeout** <*timeout*>

Mode Global Config

5.9.3.1 no tacacs-server timeout

Use the **no tacacs-server timeout** command to restore the default timeout value for all TACACS servers.

Format **no tacacs-server timeout**

Mode Global Config

5.9.4 key

Use the **key** command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon. The <*key-string*> parameter specifies the key name. For an empty string use " ". (Range: 0 - 128 characters).

Format **key** <*key-string*>

Mode TACACS Config

5.9.5 port

Use the **port** command in TACACS Configuration mode to specify a server port number. The server <*port-number*> range is 0 - 65535.

Default 49

Format **port** <*port-number*>

Mode TACACS Config

5.9.6 priority

Use the **priority** command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The <*priority*> parameter specifies the priority for servers. The highest priority is 0 (zero), and the range is 0 - 65535.

Default 0

Format **priority** <*priority*>

Mode TACACS Config

5.9.7 timeout

Use the **timeout** command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used. The <*timeout*> parameter has a range of 1-30 and is the timeout value in seconds.

Format **timeout** <*timeout*>

Mode TACACS Config

5.9.8 show tacacs

Use the **show tacacs** command to display the configuration and statistics of a TACACS+ server.

Format **show tacacs** *[<ip-address>]*

Mode Privileged EXEC

IP address The IP address of the configured TACACS+ server.

Port The configured TACACS+ server port number.

TimeOut The timeout in seconds for establishing a TCP connection.

Priority The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.

5.10 Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the **show running-config** command (see 4.3.8 “show running-config” on page 4 - 16) to capture the running configuration into a script. Use the **copy** command (see 4.5.15 “copy” on page 4 - 26) to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- The file extension must be “.scr”.
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the “!” character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access
```

```
show telnet !Displays the information about remote connections
! Display information about direct connections
show serial
! End of the script file!
```

NOTE: To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user **jane** from a blank password to **hello**, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```

5.10.1 script apply

This command applies the commands in the script to the switch. The <*scriptname*> parameter is the name of the script to apply.

Format **script apply** <*scriptname*>

Mode Privileged EXEC

5.10.2 script delete

This command deletes a specified script where the <*scriptname*> parameter is the name of the script to delete. The <*all*> option deletes all the scripts present on the switch.

Format **script delete** *{*<*scriptname*> | *all}*

Mode Privileged EXEC

5.10.3 script list

This command lists all scripts present on the switch as well as the remaining available space.

Format **script list**

Mode Global Config

Configuration Script Name of the script.

Size Privileged EXEC

5.10.4 script show

This command displays the contents of a script file, which is named <*scriptname*>.

Format **script show** <*scriptname*>

Mode Privileged EXEC

Output Format **line** <*number*>**:** <*line contents*>

5.10.5 script validate

This command validates a script file by parsing each line in the script file where <*scriptname*> is the name of the script to validate.The validate option is intended to be

used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

Format `script validate` <*scriptname*>

Mode Privileged EXEC

5.11 Pre-login Banner and System Prompt Commands

This section describes the commands you use to configure the pre-login banner and the system prompt. The pre-login banner is the text that displays before you login at the `User:` prompt.

5.11.1 copy (pre-login banner)

The `copy` command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using TFTP, Xmodem, Ymodem, or Zmodem.

Default none

Format `copy` <*tftp://<ipaddr>/<filepath>/<filename>*> `nvram:clibanner`

`copy nvram:clibanner` <*tftp://<ipaddr>/<filepath>/<filename>*>

Mode Privileged EXEC

5.11.2 set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format `set prompt` <*prompt_string*>

Mode Privileged EXEC

5.12 Watchdog Support Commands

The IPMC based hardware watchdog supervises board operation. There are 4 distinct stages in the lifecycle of the system where different watchdog timers and actions are used.

All watchdog parameters are stored in the bootloader environment. All times are in seconds. All watchdog events will power cycle the board when the watchdog expires.

- BIST watchdog during BIST
- OS loader watchdog during loading of kernel and INITRD
- Application Startup watchdog during startup of switching application
- Application Running watchdog during normal execution of switching application

5.12.1 set watchdog

This command configures the watchdog. It sets the timeout for different watchdog (during BIST, during loading of kernel and INITRD, during startup of switching application and during normal execution of switching application) and the heartbeat (sending interval and number of missed heartbeats before failure occurance). All values (except missed heartbeats) are in seconds, a value “0” means that the related watchdog is disabled.

Default disabled (0)

Format
```
set watchdog bist <0,60-6000>
set watchdog osloader <0,120-6000>
set watchdog init <0,120-6000>
set watchdog application <0,120-6000>
set watchdog heartbeat <0,1-6000>
```

Mode Privileged EXEC

5.12.2 show watchdog

This command displays the watchdog settings. It displays the values (or string "disabled") of different watchdog (during BIST, during loading of kernel and INITRD, during startup of switching application and during normal execution of switching application) and the heartbeat of the fpmux application.

Format
```
show watchdog
```

Mode Privileged EXEC

5.13 Diagnostics Commands

5.13.1 diagnostics

This command will start diagnostics. If "interactive" is specified the switch will be restarted and the diagnostics loaded. The user gets a menu to select interactively a scenario. A serial console is needed. Otherwise, if a scenario is specified, this scenario is executed directly. You may start this scenario once or repeated for a time (timedloop), for a number of repetitions (loop) or forever. The results are stored and can be displayed by using "show logging diag-report". Possible scenarios are "full" (all test purposes except the destructive ones), "quickturn" (scenarios running fast) or "write" (destructive scenarios).

Format
```
diagnostics interactive
diagnostics <scenario>
diagnostics <scenario> timedloop <1-9999999>
diagnostics <scenario> loop <1-9999999>
diagnostics <scenario> forever
```

Mode Privileged EXEC

5.13.2 copy nvram: diag-report url

This command will copy the tar.gz file containing the results of the last diagnostics run to a remote TFTP server.

Format
```
copy nvram:diag-report <url>
```

Mode Privileged EXEC

5.14 PCI express Commands

5.14.1 set board pcie upstream

This command sets the PCI Express port settings for AMC ports and update-channel port. Only one port must be upstream and only one port must be non-transparent (or

none). This ports must be specified, all not specified ports are set downstream. Below all sensible combinations are listed.

Format
```
set board pcie upstream amcb4 nt-bridge amcb2
set board pcie upstream amcb4 nt-bridge update
set board pcie upstream amcb2 nt-bridge amcb4
set board pcie upstream amcb2 nt-bridge update
set board pcie upstream amcb4
set board pcie upstream amcb2
set board pcie upstream update
```

Mode Privileged EXEC

Note: A reset of the switch is done after settings have been changed

5.14.2 set board pcie hotplug

This command enables or disables the hot-plug functionality for the specified port.

Format
```
set board pcie hotplug enable {amcb1 | amcb2 | amcb3 | amcb4}
set board pcie hotplug disable {amcb1 | amcb2 | amcb3 | amcb4}
set board pcie hotplug enable update
set board pcie hotplug disable update
```

Mode Privileged EXEC

5.14.3 set board pcie clock

This commands sets the kind of used clock. The clock can be a local SSC, local non-SSC or external clock.

Format
```
set board pcie clock ssc
set board pcie clock nssc
set board pcie clock extern
```

Mode Privileged EXEC

5.14.4 set board pcie mode

This commands sets the mode for the PCIe. The mode can be intelligent adapter mode, dual host mode or transparent mode.

Format
```
set board pcie mode adapter
set board pcie mode dual-host
set board pcie mode transparent
```

Mode Privileged EXEC

Intelligent Adapter Mode This mode allows to configure a dedicated port to be a non-transparent (NT) port. This can be useful when having an AMC module holding an additional root complex which wants to enumerate his own PCIe domain (intelligent adapter!) in addition to the root complex which is connected to the PEX8532 upstream port. This would result in 2 PCIe domains enumerated by their own root complex which are connected by the dedicated NT port. Cross-domain traffic is possible through address mapping mechanisms.

On the AT8402, any of the AMC slots or the update channel can be configured to be upstream or NT-port. Programming the address translation mapping to support the cross-domain traffic must be done by the enumerating root complex!

Dual Host Mode The dual host mode is similar to the intelligent adapter mode as any of the AMC slots or the update channel can be configured to be the upstream port or NT-port. The difference is that this mode is designed by PLX to provide a root-complex failover mechanism.

The root complex connected to the upstream port enumerates the complete PCIe domain connected to the PEX8532. This is the working root complex. The other root complex connected to the NT-port enumerates his PCIe domain stopping at the NT-port. This is the standby root complex. In the case that the working root complex fails, the standby root complex can detect this by a heartbeat mechanism. Now the standby root complex can take over the upstream port from the working root complex and continue its work without interruption. The PEX8532 provides the ability to support this switching of the upstream port.

This mode must be supported in the root complex operating systems (Re-enumeration of the PCIe hierarchy etc.).

Transparent Mode In this mode, one port is set up to be the upstream port, which is connected to the enumerating root complex. All of the other ports are fully transparent downstream ports which are connected either to PCIe end devices or additional PCIe switches/bridges.

On the AT8402, the upstream port can be programmed to be connected to any of the AMC slots or to the update channel.

5.14.5 show boardinfo pcie

This command displays the PCI Express settings. With specifying a port the setting and hot-plug function for the specified AMC port or update channel is displayed. Otherwise the command displays

- the setting (upstream, downstream or nt-bridge) and hot-plug function (enable/disable) for all AMC ports and the update-channel port.
- the kind of clock
- the PCIe mode

Format

```
show boardinfo pcie
show boardinfo pcie { amcb1 | amcb2 | amcb3 | amcb4 }
show boardinfo pcie update
```

Mode Privileged EXEC

5.15 Storage Commands

5.15.1 set board storage connect

This commands sets the connection of an AMC to a storage modul (on another AMC or on local board).

Format

```
set board storage connect amcb3 amcb1
```

```
set board storage connect amcb3 sas
set board storage connect amcb4 amcb2
set board storage connect amcb4 sas
```

Mode Privileged EXEC

5.15.2 show boardinfo storage

This commands displays information about a connection from an AMC to a storage modul.

Format
```
show boardinfo storage
show boardinfo storage amcb1
show boardinfo storage amcb3
```

Mode Privileged EXEC

5.15.3 set board sasexp program

This command sets the front plate serial interface to the SAS Expander to program the SAS Expander EEPROM.

Format
```
set board sasexp program enable
set board sasexp program disable
```

Mode Privileged Exec

5.15.4 show board sasexp program

This command displays the mode of the SAS expander programming.

Format
```
show board sasexp program
```

Mode Privileged Exec

5.16 Clock Support Commands

5.16.1 show boardinfo pll status

This command shows the PLL status.

Format
```
show boardinfo pll status
```

Mode Privileged Exec

5.16.2 show boardinfo pll config

This command shows the PLL configuration. The PLL configuration parameters are described below for the “set” command.

Format
```
show boardinfo pll config
```

Mode Privileged Exec

5.16.3 set board pll

This command shows the PLL configuration. Parameters are

- switching (manual switching/holdover switching/loss of clock)
- mode (normal operation/holdover/free run)

- filter (corner frequency 6Hz/cirener frequency 12Hz)
- select (primary clock/secondary clock)
- align (enable/disable)
- source (reference source)

Format `set board pll switching` *{manual | holdover | loss-of-clock}*
`set board pll mode` *{normal | holdover | freerun}*
`set board pll select` *{primary | secondary}*
`set board pll filter` *{6Hz | 12Hz}*
`set board pll align` *{enable | disable}*
`set board pll source` *{clk1 | clk2 | clk3}*

Mode Privileged Exec

5.16.4 show boardinfo clock bpl

This command shows the configuration of backplane clocks. The backplane clocks are displayed with the state (enabled/disabled) and (if enabled) the mapped AMC source with clock configuration attributes.

Format `show boardinfo clock bpl`

Mode Privileged Exec

5.16.5 show boardinfo clock amc

This command shows the configuration of the AMC clocks. The AMC clocks are displayed with the source (from carrier or AMC), state (enabled/disabled) and (if enabled) the internal clock index with clock configuration attributes. If the source is the AMC, it is checked whether an AMC is present (otherwise state is set to 'not present'). For source AMC the AMC is queried with the get clock state command and if the IPMI command is not supported the state is set to '--'. For source Carrier the clock state is queried from the local on-carrier device where the AMC clock is connected to.

Format `show boardinfo clock amc`

Mode Privileged Exec

5.16.6 show boardinfo clock map

This command shows the AMC sources for the backplane clocks. If no source is connected '--' is displayed.

Format `show boardinfo clock map`

Mode Privileged Exec

5.16.7 set board clock bpl

This command enables/disables a clock driver to the backplane.

Format `set board clock bpl` *{clk1a | clk1b | clk2a | clk2b | clk3a | clk3b}* `enable`
`set board clock bpl` *{clk1a | clk1b | clk2a | clk2b | clk3a | clk3b}* `disable`

Mode Privileged Exec

5.16.8 set board clock map

This command selects/deselects a source for a backplane clock. If a source is selected the attributes (frequency) must be set too. Other attributes are fixed (direction=source, family=1, accuracy=50).

Format

`set board clock map` *{clk1a | clk1b | clk2a | clk2b | clk3a | clk3b}* **`from`** *{amcb1 | amcb2 | amcb3 | amcb4} {tclkb | tclkd}* **`enable 8kHz`**

`set board clock map` *{clk1a | clk1b | clk2a | clk2b | clk3a | clk3b}* **`from`** *{amcb1 | amcb2 | amcb3 | amcb4} {tclkb | tclkd}* **`enable 1_544MHz`**

`set board clock map` *{clk1a | clk1b | clk2a | clk2b | clk3a | clk3b}* **`from`** *{amcb1 | amcb2 | amcb3 | amcb4} {tclkb | tclkd}* **`enable 2_048MHz`**

`set board clock map` *{clk1a | clk1b | clk2a | clk2b | clk3a | clk3b}* **`from`** *{amcb1 | amcb2 | amcb3 | amcb4} {tclkb | tclkd}* **`enable 19_44MHz`**

`set board clock map` *{clk1a | clk1b | clk2a | clk2b | clk3a | clk3b}* **`from`** *{amcb1 | amcb2 | amcb3 | amcb4} {tclkb | tclkd}* **`disable`**

Mode Privileged Exec





Appendix A

Getting Help

A. Getting Help

If at any time you encounter difficulties with your application or with any of our products, or if you simply need guidance on system setups and capabilities, contact our Technical Support at:

North America	EMEA
Tel.: (450) 437-5682	Tel.: +49 (0) 8341 803 xxx
Fax: (450) 437-8053	Fax: +49 (0) 8341 803 xxx

If you have any questions about Kontron, our products, or services, visit our Web site at: www.kontron.com

You also can contact us by E-mail at:

North America: support@ca.kontron.com

EMEA: support@kontron-modular.com

Or at the following address:

North America	EMEA
Kontron Canada, Inc.	Kontron Modular Computers GmbH
616 Curé Boivin	Sudetenstrasse 7
Boisbriand, Québec	87600 Kaufbeuren
J7G 2A7 Canada	Germany

RETURNING DEFECTIVE MERCHANDISE

Before returning any merchandise please do one of the following if your product malfunctions:

- **Call**

1. Call our Technical Support department in North America at (450) 437-5682 and in EMEA at +49 (0) 8341 803 xxx. Make sure you have the following on hand: our Invoice #, your Purchase Order #, and the Serial Number of the defective unit.
2. Provide the serial number found on the back of the unit and explain the nature of your problem to a service technician.
3. The technician will instruct you on the return procedure if the problem cannot be solved over the telephone.
4. Make sure you receive an RMA # from our Technical Support before returning any merchandise.

- **Fax**

1. Make a copy of the request form on the following page.
2. Fill it out.
3. Fax it to us at: North America (450) 437-0304, EMEA +49 (0) 8341 803 xxx

- **E-mail**

1. Send us an e-mail at: RMA@ca.kontron.com in North America ant at ____@_____.com in EMEA. In the e-mail, you must include your name, your company name, your address, your city, your postal/zip code, your phone number, and your e-mail. You must also include the serial number of the defective product and a description of the problem.

WHEN RETURNING A UNIT

- In the box, you have to include the name and telephone number of a person whom we can contact for further explanations if necessary when returning goods. **Where applicable, always include all duty papers and invoice(s) associated with the item(s) in question.**
- Ensure that the unit is properly packed. Pack it in a rigid cardboard box.
- Clearly write or mark the RMA number on the outside of the package you are returning.
- Ship prepaid. We take care of insuring incoming units.

North America	EMEA
Kontron Canada, Inc.	Kontron Modular Computers GmbH
616 Curé Boivin	Sudetenstrasse 7
Boisbriand, Québec	87600 Kaufbeuren
J7G 2A7 Canada	Germany

kontron

Return to Manufacturer Authorization Request

Contact Name:	_____		
Company Name:	_____		
Street Address:	_____		
City:	_____	Province/State:	_____
Country:	_____	Postal/Zip Code:	_____
Phone Number:	_____	Extension:	_____
Fax Number:	_____	E-Mail:	_____

Serial Number	Failure or Problem Description	P.O. # (if not under warranty)

Fax this form to Kontron's Technical Support department in North America at (450) 437-0304 and in EMEA at +49 (0)8341 803 XXX

Appendix B

List of Commands

B. List of Commands

{deny | permit} ..... 3 - 21
access-list ..... 3 - 24
acl-trapflags ..... 3 - 26
addport ..... 2 - 52
assign-queue ..... 3 - 12
authentication login ..... 2 - 37
auto-negotiate ..... 2 - 2
auto-negotiate all ..... 2 - 3
block ..... 2 - 5
bootfile ..... 4 - 35
bridge aging-time ..... 2 - 78
class ..... 3 - 13
class-map ..... 3 - 8
class-map rename ..... 3 - 8
classofservice dot1p-mapping ..... 3 - 2
classofservice ip-dscp-mapping ..... 3 - 3
classofservice trust ..... 3 - 3
clear board event-log ..... 4 - 23
clear config ..... 4 - 24
clear counters ..... 4 - 24
clear dot1x statistics ..... 2 - 38
clear igmpsnooping ..... 4 - 24
clear ip dhcp binding ..... 4 - 39
clear ip dhcp conflict ..... 4 - 39
clear ip dhcp server statistics ..... 4 - 39
clear lldp remote-data ..... 2 - 71
clear lldp statistics ..... 2 - 71
clear pass ..... 4 - 24
clear port-channel ..... 4 - 25
clear radius statistics ..... 2 - 38
clear traplog ..... 4 - 25
clear vlan ..... 4 - 25
CLI Error Messages ..... 1 - 8
CLI Line-Editing Conventions ..... 1 - 8
client-identifier ..... 4 - 32
client-name ..... 4 - 33
Command Completion and Abbreviation ..... 1 - 7
Common Parameter Values ..... 1 - 3
configuration ..... 5 - 5
conform-color ..... 3 - 12
copy ..... 4 - 26
copy (pre-login banner) ..... 5 - 33
copy nvram: diag-report url ..... 5 - 34
cos-queue min-bandwidth ..... 3 - 3
cos-queue strict ..... 3 - 4

debug clear ....4 - 43
debug console ....4 - 43
debug igmpsnooping packet ....4 - 47
debug igmpsnooping packet receive ....4 - 46
debug igmpsnooping packet transmit ....4 - 45
debug lacp packet ....4 - 50
debug ospf packet ....4 - 49
debug ping packet ....4 - 47
debug rip packet ....4 - 48
debug spanning-tree bpdu ....4 - 45
debug spanning-tree bpdu receive ....4 - 44
debug spanning-tree bpdu transmit ....4 - 43
default-router ....4 - 33
deleteport (Global Config) ....2 - 53
deleteport (Interface Config) ....2 - 53
description ....2 - 3
diagnostics ....5 - 34
diffserv ....3 - 7
disconnect ....5 - 9
dns-server ....4 - 33
domain-name ....4 - 35
dos-control firstfrag ....2 - 75
dos-control icmp ....2 - 77
dos-control l4port ....2 - 76
dos-control sipdip ....2 - 75
dos-control tcpflag ....2 - 76
dos-control tcpfrag ....2 - 76
dot1x defaultlogin ....2 - 39
dot1x initialize ....2 - 39
dot1x login ....2 - 39
dot1x max-req ....2 - 39
dot1x port-control ....2 - 40
dot1x port-control all ....2 - 40
dot1x re-authenticate ....2 - 40
dot1x re-authentication ....2 - 41
dot1x system-auth-control ....2 - 41
dot1x timeout ....2 - 41
dot1x user ....2 - 42
download amcipmifw ....4 - 3
download bootloader ....4 - 3
download frudata ....4 - 2
download fwum ....4 - 3
download initrd ....4 - 2
download ipmifw ....4 - 2
drop ....3 - 12
dvlan-tunnel ethertype ....2 - 28

ekeying (interface) ..... 4 - 5
enable (Privileged EXEC access) ..... 5 - 2
enable passwd ..... 4 - 25
hardware-address ..... 4 - 34
host ..... 4 - 34
interface ..... 2 - 2
ip access-group ..... 3 - 25
ip dhcp bootp automatic ..... 4 - 38
ip dhcp conflict logging ..... 4 - 39
ip dhcp excluded-address ..... 4 - 37
ip dhcp filtering ..... 4 - 42
ip dhcp filtering trust ..... 4 - 42
ip dhcp ping packets ..... 4 - 38
ip dhcp pool ..... 4 - 32
ip ssh ..... 5 - 10
ip ssh protocol ..... 5 - 11
ip ssh server enable ..... 5 - 11
ip telnet server enable ..... 5 - 6
key ..... 5 - 30
lease ..... 4 - 34
license advanced ..... 4 - 27
lineconfig ..... 5 - 5
lldp notification ..... 2 - 70
lldp notification-interval ..... 2 - 71
lldp receive ..... 2 - 69
lldp timers ..... 2 - 69
lldp transmit ..... 2 - 69
lldp transmit-mgmt ..... 2 - 70
lldp transmit-tlv ..... 2 - 70
logging buffered ..... 4 - 20
logging buffered wrap ..... 4 - 20
logging cli-command ..... 4 - 20
logging cli-command ..... 5 - 23
logging console ..... 4 - 20
logging host ..... 4 - 21
logging host remove ..... 4 - 21
logging port ..... 4 - 21
logging syslog ..... 4 - 22
logout ..... 4 - 25
mac access-group ..... 3 - 22
mac access-list extended ..... 3 - 21
mac access-list extended rename ..... 3 - 21
macfilter ..... 2 - 58
macfilter addsrc ..... 2 - 59
macfilter addsrc all ..... 2 - 59
mark cos ..... 3 - 13

mark ip-dscp ..... 3 - 13
mark ip-precedence ..... 3 - 14
match any ..... 3 - 8
match class-map ..... 3 - 9
match dstip ..... 3 - 9
match dstl4port ..... 3 - 9
match ip dscp ..... 3 - 10
match ip precedence ..... 3 - 10
match ip tos ..... 3 - 10
match protocol ..... 3 - 11
match srcip ..... 3 - 11
match srcl4port ..... 3 - 11
mode dot1q-tunnel ..... 2 - 28
mode dvlan-tunnel ..... 2 - 28
monitor session ..... 2 - 57
mtu ..... 2 - 3
netbios-name-server ..... 4 - 36
netbios-node-type ..... 4 - 36
network (DHCP Pool Config) ..... 4 - 35
network mac-address ..... 5 - 3
network mac-type ..... 5 - 3
network mgmt_vlan ..... 2 - 18
network parms ..... 5 - 3
network protocol ..... 5 - 3
next-server ..... 4 - 36
no access-list ..... 3 - 25
no acl-trapflags ..... 3 - 26
no authentication login ..... 2 - 38
no auto-negotiate all ..... 2 - 3
no auto-negotiate ..... 2 - 3
no block ..... 2 - 5
no bootfile ..... 4 - 35
no bridge aging-time ..... 2 - 78
no class ..... 3 - 13
no class-map ..... 3 - 8
no classofservice dot1p-mapping ..... 3 - 2
no classofservice ip-dscp-mapping ..... 3 - 3
no classofservice trust ..... 3 - 3
no client-identifier ..... 4 - 32
no client-name ..... 4 - 33
no cos-queue min-bandwidth ..... 3 - 4
no cos-queue strict ..... 3 - 4
no debug console ..... 4 - 43
no debug igmpsnooping packet ..... 4 - 47
no debug igmpsnooping receive ..... 4 - 46
no debug igmpsnooping transmit ..... 4 - 46

no debug lacp packet ..... 4 - 50
no debug ospf packet ..... 4 - 50
no debug ping packet ..... 4 - 47
no debug rip packet ..... 4 - 48
no debug spanning-tree bpdu receive ..... 4 - 45
no debug spanning-tree bpdu transmit ..... 4 - 44
no debug spanning-tree bpdu ..... 4 - 45
no default-router ..... 4 - 33
no diffserv ..... 3 - 7
no dns-server ..... 4 - 33
no domain-name ..... 4 - 35
no dos-control firstfrag ..... 2 - 75
no dos-control icmp ..... 2 - 77
no dos-control l4port ..... 2 - 77
no dos-control sipdip ..... 2 - 75
no dos-control tcpflag ..... 2 - 76
no dos-control tcpfrag ..... 2 - 76
no dot1x max-req ..... 2 - 39
no dot1x port-control all ..... 2 - 40
no dot1x port-control ..... 2 - 40
no dot1x re-authentication ..... 2 - 41
no dot1x system-auth-control ..... 2 - 41
no dot1x timeout ..... 2 - 42
no dot1x user ..... 2 - 42
no ekeying (interface) ..... 4 - 5
no hardware-address ..... 4 - 34
no host ..... 4 - 34
no ip access-group ..... 3 - 25
no ip dhcp bootp automatic ..... 4 - 38
no ip dhcp conflict logging ..... 4 - 39
no ip dhcp excluded-address ..... 4 - 37
no ip dhcp filtering trust ..... 4 - 42
no ip dhcp filtering ..... 4 - 42
no ip dhcp ping packets ..... 4 - 38
no ip dhcp pool ..... 4 - 32
no ip ssh server enable ..... 5 - 11
no ip ssh ..... 5 - 11
no ip telnet server enable ..... 5 - 7
no lease ..... 4 - 35
no license advanced ..... 4 - 28
no lldp notification ..... 2 - 71
no lldp notification-interval ..... 2 - 71
no lldp receive ..... 2 - 69
no lldp timers ..... 2 - 70
no lldp transmit ..... 2 - 69
no lldp transmit-mgmt ..... 2 - 70

no lldp transmit-tlv ..... 2 - 70
no logging buffered wrap ..... 4 - 20
no logging buffered ..... 4 - 20
no logging cli-command ..... 4 - 20
no logging cli-command ..... 5 - 23
no logging console ..... 4 - 21
no logging port ..... 4 - 21
no logging syslog ..... 4 - 22
no mac access-group ..... 3 - 23
no mac access-list extended ..... 3 - 21
no macfilter addsrc all ..... 2 - 59
no macfilter addsrc ..... 2 - 59
no macfilter ..... 2 - 58
no match class-map ..... 3 - 9
no mode dot1q-tunnel ..... 2 - 28
no mode dvlan-tunnel ..... 2 - 28
no monitor ..... 2 - 57
no monitor session ..... 2 - 57
no mtu ..... 2 - 3
no netbios-name-server ..... 4 - 36
no netbios-node-type ..... 4 - 36
no network mac-type ..... 5 - 4
no network mgmt_vlan ..... 2 - 18
no network ..... 4 - 35
no next-server ..... 4 - 37
no option ..... 4 - 37
no policy-map ..... 3 - 15
no port lacp timeout ..... 2 - 54
no port lacp timeout ..... 2 - 54
no port lacpmode all ..... 2 - 54
no port lacpmode ..... 2 - 54
no port-channel adminmode ..... 2 - 55
no port-channel linktrap ..... 2 - 55
no port-channel static ..... 2 - 53
no port-channel ..... 2 - 52
no port-security mac-address ..... 2 - 67
no port-security max-dynamic ..... 2 - 67
no port-security max-static ..... 2 - 67
no port-security ..... 2 - 66
no protocol group ..... 2 - 23
no protocol vlan group all ..... 2 - 24
no protocol vlan group ..... 2 - 23
no radius accounting mode ..... 5 - 24
no radius server host ..... 5 - 24
no radius server msgauth ..... 5 - 25
no radius server retransmit ..... 5 - 26

no radius server timeout ..... 5 - 26
no serial baudrate ..... 5 - 5
no serial timeout ..... 5 - 6
no service dhcp ..... 4 - 38
no service-policy ..... 3 - 16
no session-limit ..... 5 - 8
no session-timeout ..... 5 - 8
no set bootstopkey ..... 4 - 25
no set garp timer join ..... 2 - 32
no set garp timer leave ..... 2 - 33
no set garp timer leaveall ..... 2 - 33
no set gmrp adminmode ..... 2 - 36
no set gmrp interfacemode ..... 2 - 36
no set gvrp adminmode ..... 2 - 34
no set gvrp interfacemode ..... 2 - 34
no set igmp fast-leave ..... 2 - 62
no set igmp groupmembership-interval ..... 2 - 62
no set igmp interfacemode ..... 2 - 61
no set igmp maxresponse ..... 2 - 63
no set igmp mcrtexpiretime ..... 2 - 63
no set igmp mrouter interface ..... 2 - 64
no set igmp mrouter ..... 2 - 64
no set igmp ..... 2 - 61
no shutdown all ..... 2 - 4
no shutdown ..... 2 - 4
no snmp trap link-status all ..... 5 - 21
no snmp trap link-status ..... 5 - 21
no snmp-server community ipaddr ..... 5 - 16
no snmp-server community ipmask ..... 5 - 17
no snmp-server community mode ..... 5 - 17
no snmp-server community ..... 5 - 16
no snmp-server enable traps bcaststorm ..... 5 - 18
no snmp-server enable traps linkmode ..... 5 - 19
no snmp-server enable traps multiusers ..... 5 - 19
no snmp-server enable traps stpmode ..... 5 - 19
no snmp-server enable traps violation ..... 5 - 18
no snmp-server enable traps ..... 5 - 18
no snmptrap mode ..... 5 - 21
no snmptrap ..... 5 - 20
no sntp broadcast client poll-interval ..... 4 - 28
no sntp client mode ..... 4 - 29
no sntp client port ..... 4 - 29
no sntp multicast client poll-interval ..... 4 - 30
no sntp server ..... 4 - 30
no sntp unicast client poll-interval ..... 4 - 29
no sntp unicast client poll-retry ..... 4 - 30

no sntp unicast client poll-timeout ..... 4 - 29
no spanning-tree configuration name ..... 2 - 7
no spanning-tree configuration revision ..... 2 - 7
no spanning-tree edgeport ..... 2 - 8
no spanning-tree forceversion ..... 2 - 8
no spanning-tree forward-time ..... 2 - 8
no spanning-tree hello-time ..... 2 - 9
no spanning-tree max-age ..... 2 - 9
no spanning-tree max-hops ..... 2 - 9
no spanning-tree mst instance ..... 2 - 11
no spanning-tree mst priority ..... 2 - 11
no spanning-tree mst vlan ..... 2 - 12
no spanning-tree mst ..... 2 - 10
no spanning-tree port mode all ..... 2 - 13
no spanning-tree port mode ..... 2 - 12
no spanning-tree ..... 2 - 6
no sshcon maxsessions ..... 5 - 11
no sshcon timeout ..... 5 - 12
no storm-control broadcast all level ..... 2 - 48
no storm-control broadcast all ..... 2 - 47
no storm-control broadcast level ..... 2 - 47
no storm-control broadcast ..... 2 - 46
no storm-control flowcontrol ..... 2 - 51
no storm-control multicast all level ..... 2 - 49
no storm-control multicast all ..... 2 - 49
no storm-control multicast level ..... 2 - 48
no storm-control multicast ..... 2 - 48
no storm-control unicast all level ..... 2 - 51
no storm-control unicast all ..... 2 - 50
no storm-control unicast level ..... 2 - 50
no storm-control unicast ..... 2 - 49
no switchport protected (Global Config) ..... 2 - 31
no switchport protected (Interface Config) ..... 2 - 31
no tacacs-server host ..... 5 - 29
no tacacs-server key ..... 5 - 29
no tacacs-server timeout ..... 5 - 30
no telnetcon maxsessions ..... 5 - 9
no telnetcon timeout ..... 5 - 9
no traffic-shape ..... 3 - 4
no transport input telnet ..... 5 - 7
no transport output telnet ..... 5 - 8
no users name ..... 5 - 13
no users passwd ..... 5 - 13
no users snmpv3 accessmode ..... 5 - 14
no users snmpv3 authentication ..... 5 - 14
no users snmpv3 encryption ..... 5 - 15

no vlan acceptframe ..... 2 - 18
no vlan association mac ..... 2 - 25
no vlan association subnet ..... 2 - 25
no vlan ingressfilter ..... 2 - 19
no vlan name ..... 2 - 19
no vlan port acceptframe all ..... 2 - 20
no vlan port ingressfilter all ..... 2 - 21
no vlan port pvid all ..... 2 - 21
no vlan port tagging all ..... 2 - 22
no vlan protocol group add protocol ..... 2 - 22
no vlan pvid ..... 2 - 24
no vlan tagging ..... 2 - 24
no vlan ..... 2 - 18
option ..... 4 - 37
ping ..... 4 - 26
police-simple ..... 3 - 14
policy-map ..... 3 - 14
policy-map rename ..... 3 - 15
port ..... 5 - 30
port lacp timeout (Global Config) ..... 2 - 54
port lacp timeout (Interface Config) ..... 2 - 54
port lacpmode ..... 2 - 53
port lacpmode all ..... 2 - 54
port-channel ..... 2 - 52
port-channel adminmode ..... 2 - 55
port-channel linktrap ..... 2 - 55
port-channel name ..... 2 - 55
port-channel static ..... 2 - 53
port-security ..... 2 - 66
port-security mac-address ..... 2 - 67
port-security mac-address move ..... 2 - 68
port-security max-dynamic ..... 2 - 67
port-security max-static ..... 2 - 67
priority ..... 5 - 30
protocol group ..... 2 - 23
protocol vlan group ..... 2 - 23
protocol vlan group all ..... 2 - 23
quit ..... 4 - 26
radius accounting mode ..... 5 - 24
radius server host ..... 5 - 24
radius server key ..... 5 - 25
radius server msgauth ..... 5 - 25
radius server primary ..... 5 - 25
radius server retransmit ..... 5 - 25
radius server timeout ..... 5 - 26
reload ..... 4 - 26

script apply ....5 - 32
script delete ....5 - 32
script list ....5 - 32
script show ....5 - 32
script validate ....5 - 32
serial baudrate ....5 - 5
serial timeout ....5 - 6
service dhcp ....4 - 38
service-policy ....3 - 15
serviceport ip ....5 - 2
serviceport protocol ....5 - 3
session-limit ....5 - 8
session-timeout ....5 - 8
set board bootcycle ....4 - 5
set board clock bpl ....5 - 38
set board clock map ....5 - 39
set board device-id ....4 - 4
set board fcap ....4 - 4
set board ipmi-controller debug ....4 - 4
set board pcie clock ....5 - 35
set board pcie hotplug ....5 - 35
set board pcie mode ....5 - 35
set board pcie upstream ....5 - 34
set board pll ....5 - 37
set board sasexp program ....5 - 37
set board sensor threshold ....4 - 4
set board storage connect ....5 - 36
set bootstopkey ....4 - 25
set garp timer join ....2 - 32
set garp timer leave ....2 - 32
set garp timer leaveall ....2 - 33
set gmrp adminmode ....2 - 35
set gmrp interfacemode ....2 - 36
set gvrp adminmode ....2 - 34
set gvrp interfacemode ....2 - 34
set igmp ....2 - 60
set igmp fast-leave ....2 - 61
set igmp groupmembership-interval ....2 - 62
set igmp interfacemode ....2 - 61
set igmp maxresponse ....2 - 62
set igmp mcrtexpiretime ....2 - 63
set igmp mrouter ....2 - 63
set igmp mrouter interface ....2 - 64
set prompt ....5 - 33
set watchdog ....5 - 33
show access-lists ....3 - 27

show arp switch ..... 4 - 6
show atca ekeying ..... 4 - 5
show authentication ..... 2 - 43
show authentication users ..... 2 - 43
show board sasexp program ..... 5 - 37
show boardinfo address ..... 4 - 18
show boardinfo amc connection ..... 4 - 19
show boardinfo amc fru ..... 4 - 19
show boardinfo amc ipmidev ..... 4 - 19
show boardinfo bootcycle ..... 4 - 19
show boardinfo clock amc ..... 5 - 38
show boardinfo clock bpl ..... 5 - 38
show boardinfo clock map ..... 5 - 38
show boardinfo event-log ..... 4 - 17
show boardinfo fcap ..... 4 - 19
show boardinfo fru ..... 4 - 18
show boardinfo ipmidev ..... 4 - 18
show boardinfo led ..... 4 - 18
show boardinfo pcie ..... 5 - 36
show boardinfo pll config ..... 5 - 37
show boardinfo pll status ..... 5 - 37
show boardinfo post-status ..... 4 - 17
show boardinfo sensors ..... 4 - 17
show boardinfo storage ..... 5 - 37
show boardinfo update-status ..... 4 - 17
show boardinfo version ..... 4 - 18
show class-map ..... 3 - 16
show classofservice dot1p-mapping ..... 3 - 4
show classofservice ip-dscp-mapping ..... 3 - 5
show classofservice ip-precedence-mapping ..... 3 - 5
show classofservice trust ..... 3 - 5
show diffserv ..... 3 - 17
show diffserv service ..... 3 - 19
show diffserv service brief ..... 3 - 19
show dos-control ..... 2 - 77
show dot1q-tunnel ..... 2 - 29
show dot1x ..... 2 - 43
show dot1x users ..... 2 - 46
show dvlan-tunnel ..... 2 - 29
show eventlog ..... 4 - 6
show forwardingdb agetime ..... 2 - 78
show garp ..... 2 - 33
show gmrp configuration ..... 2 - 36
show gvrp configuration ..... 2 - 34
show hardware ..... 4 - 6
show igmpsnooping ..... 2 - 64

show igmpsnooping mrouter interface ....2 - 65
show igmpsnooping mrouter vlan ....2 - 65
show interface ....4 - 7
show interface ethernet ....4 - 8
show interfaces cos-queue ....3 - 6
show interfaces switchport ....2 - 31
show ip access-lists ....3 - 26
show ip dhcp binding ....4 - 39
show ip dhcp conflict ....4 - 41
show ip dhcp filtering ....4 - 42
show ip dhcp global configuration ....4 - 40
show ip dhcp pool configuration ....4 - 40
show ip dhcp server statistics ....4 - 41
show ip ssh ....5 - 12
show key-features ....4 - 28
show lldp ....2 - 71
show lldp interface ....2 - 72
show lldp local-device ....2 - 74
show lldp local-device detail ....2 - 74
show lldp remote-device ....2 - 73
show lldp remote-device detail ....2 - 73
show lldp statistics ....2 - 72
show logging ....4 - 22
show logging backtrace ....4 - 23
show logging buffered ....4 - 22
show logging diag-report ....4 - 23
show logging hosts ....4 - 23
show logging traplogs ....4 - 23
show loginsession ....5 - 9
show mac access-lists ....3 - 23
show mac-address-table gmrp ....2 - 37
show mac-address-table igmpsnooping ....2 - 66
show mac-address-table multicast ....2 - 78
show mac-address-table static ....2 - 59
show mac-address-table staticfiltering ....2 - 60
show mac-address-table stats ....2 - 79
show mac-addr-table ....4 - 15
show monitor session ....2 - 57
show network ....5 - 4
show policy-map ....3 - 17
show policy-map interface ....3 - 20
show port ....2 - 5
show port protocol ....2 - 6
show port-channel ....2 - 56
show port-channel brief ....2 - 55
show port-security ....2 - 68

show port-security dynamic ..... 2 - 68
show port-security static ..... 2 - 68
show port-security violation ..... 2 - 68
show radius ..... 5 - 26
show radius accounting ..... 5 - 27
show radius statistics ..... 5 - 28
show running-config ..... 4 - 16
show serial ..... 5 - 6
show service-policy ..... 3 - 20
show serviceport ..... 5 - 4
show snmpcommunity ..... 5 - 21
show snmptrap ..... 5 - 22
show sntp ..... 4 - 30
show sntp client ..... 4 - 31
show sntp server ..... 4 - 31
show spanning-tree ..... 2 - 13
show spanning-tree brief ..... 2 - 14
show spanning-tree interface ..... 2 - 14
show spanning-tree mst port detailed ..... 2 - 15
show spanning-tree mst port summary ..... 2 - 16
show spanning-tree mst summary ..... 2 - 16
show spanning-tree summary ..... 2 - 17
show spanning-tree vlan ..... 2 - 17
show startupconfig ..... 4 - 4
show storm-control ..... 2 - 51
show switchport protected ..... 2 - 31
show sysinfo ..... 4 - 16
show tacacs ..... 5 - 31
show tech-support ..... 4 - 17
show telnet ..... 5 - 10
show telnetcon ..... 5 - 10
show trapflags ..... 5 - 22
show users ..... 5 - 15
show users authentication ..... 2 - 46
show version ..... 4 - 6
show vlan ..... 2 - 25
show vlan association mac ..... 2 - 27
show vlan association subnet ..... 2 - 27
show vlan brief ..... 2 - 26
show vlan port ..... 2 - 26
show watchdog ..... 5 - 34
shutdown ..... 2 - 4
shutdown all ..... 2 - 4
snmp trap link-status ..... 5 - 21
snmp trap link-status all ..... 5 - 21
snmp-server ..... 5 - 15

snmp-server community ....5 - 16
snmp-server community ipaddr ....5 - 16
snmp-server community ipmask ....5 - 16
snmp-server community mode ....5 - 17
snmp-server community ro ....5 - 17
snmp-server community rw ....5 - 17
snmp-server enable traps ....5 - 18
snmp-server enable traps bcaststorm ....5 - 18
snmp-server enable traps linkmode ....5 - 19
snmp-server enable traps multiusers ....5 - 19
snmp-server enable traps stpmode ....5 - 19
snmp-server enable traps violation ....5 - 18
snmptrap ....5 - 20
snmptrap ipaddr ....5 - 20
snmptrap mode ....5 - 20
snmptrap snmpversion ....5 - 20
sntp broadcast client poll-interval ....4 - 28
sntp client mode ....4 - 28
sntp client port ....4 - 29
sntp multicast client poll-interval ....4 - 30
sntp server ....4 - 30
sntp unicast client poll-interval ....4 - 29
sntp unicast client poll-retry ....4 - 30
sntp unicast client poll-timeout ....4 - 29
spanning-tree ....2 - 6
spanning-tree bpdumigrationcheck ....2 - 7
spanning-tree configuration name ....2 - 7
spanning-tree configuration revision ....2 - 7
spanning-tree edgeport ....2 - 8
spanning-tree forceversion ....2 - 8
spanning-tree forward-time ....2 - 8
spanning-tree hello-time ....2 - 9
spanning-tree max-age ....2 - 9
spanning-tree max-hops ....2 - 9
spanning-tree mst ....2 - 10
spanning-tree mst instance ....2 - 11
spanning-tree mst priority ....2 - 11
spanning-tree mst vlan ....2 - 12
spanning-tree port mode ....2 - 12
spanning-tree port mode all ....2 - 12
speed ....2 - 4
speed all ....2 - 5
sshcon maxsessions ....5 - 11
sshcon timeout ....5 - 12
startupslot ....4 - 3
startupslot activate ....4 - 3

storm-control broadcast ..... 2 - 46
storm-control broadcast all ..... 2 - 47
storm-control broadcast all level ..... 2 - 47
storm-control broadcast level ..... 2 - 47
storm-control flowcontrol ..... 2 - 51
storm-control multicast ..... 2 - 48
storm-control multicast all ..... 2 - 48
storm-control multicast all level ..... 2 - 49
storm-control multicast level ..... 2 - 48
storm-control unicast ..... 2 - 49
storm-control unicast all ..... 2 - 50
storm-control unicast all level ..... 2 - 50
storm-control unicast level ..... 2 - 50
switchport protected (Global Config) ..... 2 - 30
switchport protected (Interface Config) ..... 2 - 31
tacacs-server host ..... 5 - 29
tacacs-server key ..... 5 - 29
tacacs-server timeout ..... 5 - 30
telnet ..... 5 - 7
telnetcon maxsessions ..... 5 - 8
telnetcon timeout ..... 5 - 9
timeout ..... 5 - 31
traceroute ..... 4 - 24
traffic-shape ..... 3 - 4
transport input telnet ..... 5 - 7
transport output telnet ..... 5 - 7
users defaultlogin ..... 2 - 42
users login ..... 2 - 43
users name ..... 5 - 12
users passwd ..... 5 - 13
users snmpv3 accessmode ..... 5 - 13
users snmpv3 authentication ..... 5 - 14
users snmpv3 encryption ..... 5 - 14
vlan ..... 2 - 18
vlan acceptframe ..... 2 - 18
vlan association mac ..... 2 - 25
vlan association subnet ..... 2 - 24
vlan database ..... 2 - 17
vlan ingressfilter ..... 2 - 19
vlan makestatic ..... 2 - 19
vlan name ..... 2 - 19
vlan participation ..... 2 - 19
vlan participation all ..... 2 - 20
vlan port acceptframe all ..... 2 - 20
vlan port ingressfilter all ..... 2 - 21
vlan port priority all ..... 2 - 30

vlan port pvid all .....2 - 21
vlan port tagging all .....2 - 21
vlan priority .....2 - 30
vlan protocol group .....2 - 22
vlan protocol group add protocol .....2 - 22
vlan protocol group remove .....2 - 22
vlan pvid .....2 - 24
vlan tagging .....2 - 24

