AM4904/AM4910 CLI Reference Manual

MicroTCA Carrier Hub

S1100_TECH_2	Manual ID
2.04	Revision Index
March 16, 2012	Date of Issue

Revision History

Publication Title:	S1100 CLI Reference Manual	
ID Number:	S1100_TECH_2	
Rev. Index	**Brief Description of Changes**	**Date of Issue**
2.00	First version	19 Oct., 2009
2.01	Added sfp/sfp+ commands, added DHCP force-client-id commands, added chkconfig commands, added 'copy <url> all-config' command	03 May, 2010
2.02	Updated with support for IP routing and Multicast	20 May, 2011
2.03	Updated with missing commands, corrections, removals	28. Oct, 2011
2.04	Updated with new commands (copy <url> ipmi-hpm) and command updates (protection-group, macfilter)	March 16, 2012

Imprint

Kontron AG may be contacted via the following:

	North America	**EMEA**
	Kontron Canada, Inc.	Kontron Modular Computers GmbH
	4555 Ambroise-Lafortune	Sudetenstrasse 7
	Boisbriand, Québec	87600 Kaufbeuren
	J7H 0A4 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.

About This Book

This document describes command-line interface (CLI) commands you use to view and configure FASTPATH software. You can access the CLI by using a direct connection to the serial port or by using telnet or SSH over a remote network connection.

This document is for system administrators who configure and operate systems using FASTPATH software. It provides an understanding of the configuration options of the FASTPATH software.

Software engineers who integrate FASTPATH software into their hardware platform can also benefit from a description of the configuration options.

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

How to Use This Document

Chapter 1 “Using the Command-Line Interface” 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

Broadcom®, the pulse logo, Connecting everything®, the Connecting everything logo, and FASTPATH® are among the trademarks of Broadcom Corporation and/or its affiliates in the United States, certain other countries and/or the EU. Any other trademarks or trade names mentioned 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.

Revision History ii
Imprint ii
Disclaimer ii
About This Book iii
How to Use This Document iii
Proprietary Note iii
Trademarks iii
Environmental Protection Statement iv
Explanation of Symbols iv
For Your Safety iv
High Voltage Safety Instructions iv
Special Handling and Unpacking Instructions v
General Instructions on Usage v
Two Year Warranty v

Chapter 1

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

Chapter 2

2. Switching Commands ..... 2 - 2

2.1 Port Configuration Commands ....2 - 3
2.1.1 interface ....2 - 3
2.1.2 auto-negotiate ....2 - 3
2.1.3 auto-negotiate all ....2 - 3
2.1.4 advertise speed ....2 - 4
2.1.5 show advertise speed ....2 - 4
2.1.6 block ....2 - 4
2.1.7 description ....2 - 4
2.1.8 mtu ....2 - 5
2.1.9 shutdown ....2 - 5
2.1.10 shutdown all ....2 - 5
2.1.11 speed ....2 - 6
2.1.12 speed all ....2 - 6
2.1.13 show port ....2 - 6
2.1.14 show port protocol ....2 - 7
2.2 Spanning Tree Protocol (STP) Commands ....2 - 7
2.2.1 spanning-tree ....2 - 7
2.2.2 spanning-tree bpdufilter ....2 - 8
2.2.3 spanning-tree bpdufilter default ....2 - 8
2.2.4 spanning-tree bpduflood ....2 - 8
2.2.5 spanning-tree bpduguard ....2 - 9
2.2.6 spanning-tree bpdumigrationcheck ....2 - 9
2.2.7 spanning-tree configuration name ....2 - 9
2.2.8 spanning-tree configuration revision ....2 - 10
2.2.9 spanning-tree edgeport ....2 - 10
2.2.10 spanning-tree forceversion ....2 - 10
2.2.11 spanning-tree forward-time ....2 - 11
2.2.12 spanning-tree guard ....2 - 11
2.2.13 spanning-tree max-age ....2 - 11
2.2.14 spanning-tree max-hops ....2 - 12
2.2.15 spanning-tree mst ....2 - 12
2.2.16 spanning-tree mst instance ....2 - 13
2.2.17 spanning-tree mst priority ....2 - 14
2.2.18 spanning-tree mst vlan ....2 - 14
2.2.19 spanning-tree port mode ....2 - 14
2.2.20 spanning-tree port mode all ....2 - 15
2.2.21 spanning-tree port-state ....2 - 15
2.2.22 show spanning-tree ....2 - 15
2.2.23 show spanning-tree brief ....2 - 16
2.2.24 show spanning-tree interface ....2 - 17
2.2.25 show spanning-tree mst port detailed ....2 - 17
2.2.26 show spanning-tree mst port summary ....2 - 19
2.2.27 show spanning-tree mst summary ....2 - 19
2.2.28 show spanning-tree summary ....2 - 20
2.2.29 show spanning-tree vlan ....2 - 20
2.3 VLAN Commands ....2 - 20

2.3.1 vlan database ..... 2 - 21
2.3.2 network mgmt_vlan ..... 2 - 21
2.3.3 vlan ..... 2 - 21
2.3.4 vlan acceptframe ..... 2 - 21
2.3.5 vlan ingressfilter ..... 2 - 22
2.3.6 vlan makestatic ..... 2 - 22
2.3.7 vlan name ..... 2 - 22
2.3.8 vlan participation ..... 2 - 23
2.3.9 vlan participation all ..... 2 - 23
2.3.10 vlan port acceptframe all ..... 2 - 23
2.3.11 vlan port ingressfilter all ..... 2 - 24
2.3.12 vlan port pvid all ..... 2 - 24
2.3.13 vlan port tagging all ..... 2 - 25
2.3.14 vlan protocol group ..... 2 - 25
2.3.15 vlan protocol group add protocol ..... 2 - 25
2.3.16 vlan protocol group remove ..... 2 - 26
2.3.17 protocol group ..... 2 - 26
2.3.18 protocol vlan group ..... 2 - 26
2.3.19 protocol vlan group all ..... 2 - 26
2.3.20 vlan pvid ..... 2 - 27
2.3.21 vlan tagging ..... 2 - 27
2.3.22 vlan association subnet ..... 2 - 27
2.3.23 vlan association mac ..... 2 - 28
2.3.24 show vlan ..... 2 - 28
2.3.25 show vlan brief ..... 2 - 29
2.3.26 show vlan port ..... 2 - 29
2.3.27 show vlan association subnet ..... 2 - 30
2.3.28 show vlan association mac ..... 2 - 30
2.4 Double VLAN Commands ..... 2 - 30
2.4.1 dvlan-tunnel ethertype (Global Config) ..... 2 - 30
2.4.2 dvlan-tunnel ethertype default-tpid ..... 2 - 31
2.4.3 mode dot1q-tunnel ..... 2 - 31
2.4.4 mode dvlan-tunnel ..... 2 - 32
2.4.5 show dot1q-tunnel ..... 2 - 32
2.4.6 show dvlan-tunnel ..... 2 - 33
2.5 Voice VLAN Commands ..... 2 - 33
2.5.1 voice vlan (Global Config) ..... 2 - 33
2.5.2 voice vlan (Interface Config) ..... 2 - 34
2.5.3 voice vlan data priority ..... 2 - 34
2.5.4 show voice vlan ..... 2 - 34
2.6 Provisioning (IEEE 802.1p) Commands ..... 2 - 36
2.6.1 vlan port priority all ..... 2 - 36
2.6.2 vlan priority ..... 2 - 37
2.7 Protected Ports Commands ..... 2 - 37
2.7.1 switchport protected (Global Config) ..... 2 - 37

2.7.2 switchport protected (Interface Config) ....2 - 37
2.7.3 show switchport protected ....2 - 38
2.7.4 show interfaces switchport ....2 - 38
2.8 GARP Commands ....2 - 39
2.8.1 set garp timer join ....2 - 39
2.8.2 set garp timer leave ....2 - 39
2.8.3 set garp timer leaveall ....2 - 40
2.8.4 show garp ....2 - 40
2.9 GVRP Commands ....2 - 40
2.9.1 set gvrp adminmode ....2 - 40
2.9.2 set gvrp interfacemode ....2 - 41
2.9.3 show gvrp configuration ....2 - 41
2.10 GMRP Commands ....2 - 42
2.10.1 set gmrp adminmode ....2 - 42
2.10.2 set gmrp interfacemode ....2 - 42
2.10.3 show gmrp configuration ....2 - 43
2.10.4 show mac-address-table gmrp ....2 - 43
2.11 Port-Based Network Access Control Commands ....2 - 44
2.11.1 authentication login ....2 - 44
2.11.2 clear dot1x statistics ....2 - 45
2.11.3 clear radius statistics ....2 - 45
2.11.4 dot1x default-login ....2 - 45
2.11.5 dot1x guest-vlan ....2 - 45
2.11.6 dot1x initialize ....2 - 45
2.11.7 dot1x login ....2 - 46
2.11.8 dot1x max-req ....2 - 46
2.11.9 dot1x max-users ....2 - 46
2.11.10 dot1x port-control ....2 - 46
2.11.11 dot1x port-control all ....2 - 47
2.11.12 dot1x re-authenticate ....2 - 47
2.11.13 dot1x re-authentication ....2 - 48
2.11.14 dot1x system-auth-control ....2 - 48
2.11.15 dot1x timeout ....2 - 48
2.11.16 dot1x unauthenticated-vlan ....2 - 49
2.11.17 dot1x user ....2 - 49
2.11.18 users defaultlogin ....2 - 50
2.11.19 users login ....2 - 50
2.11.20 show authentication ....2 - 50
2.11.21 show authentication methods ....2 - 50
2.11.22 show authentication users ....2 - 51
2.11.23 show dot1x ....2 - 51
2.11.24 show dot1x clients ....2 - 54
2.11.25 show dot1x users ....2 - 55
2.12 Storm-Control Commands ....2 - 55
2.12.1 storm-control broadcast ....2 - 55

2.12.2 storm-control broadcast level ..... 2 - 56
2.12.3 storm-control broadcast rate ..... 2 - 56
2.12.4 storm-control broadcast all ..... 2 - 57
2.12.5 storm-control broadcast all level ..... 2 - 57
2.12.6 storm-control broadcast all rate ..... 2 - 57
2.12.7 storm-control multicast ..... 2 - 58
2.12.8 storm-control multicast level ..... 2 - 58
2.12.9 storm-control multicast rate ..... 2 - 58
2.12.10 storm-control multicast all ..... 2 - 59
2.12.11 storm-control multicast all level ..... 2 - 59
2.12.12 storm-control multicast all rate ..... 2 - 60
2.12.13 storm-control unicast ..... 2 - 60
2.12.14 storm-control unicast level ..... 2 - 60
2.12.15 storm-control unicast rate ..... 2 - 61
2.12.16 storm-control unicast all ..... 2 - 61
2.12.17 storm-control unicast all level ..... 2 - 62
2.12.18 storm-control unicast all rate ..... 2 - 62
2.12.19 storm-control flowcontrol (AM4910 only) ..... 2 - 62
2.12.20 storm-control flowcontrol (AM4904 only) ..... 2 - 63
2.12.21 show storm-control ..... 2 - 64
2.12.22 show storm-control flowcontrol ..... 2 - 65
2.13 Port-Channel/LAG (802.3ad) Commands ..... 2 - 65
2.13.1 port-channel ..... 2 - 65
2.13.2 addport ..... 2 - 66
2.13.3 deleteport (Interface Config) ..... 2 - 66
2.13.4 deleteport (Global Config) ..... 2 - 66
2.13.5 lacp admin key ..... 2 - 66
2.13.6 lacp collector max-delay ..... 2 - 67
2.13.7 lacp actor admin ..... 2 - 67
2.13.8 lacp actor admin key ..... 2 - 67
2.13.9 lacp actor admin state ..... 2 - 68
2.13.10 lacp actor admin state individual ..... 2 - 68
2.13.11 lacp actor admin state longtimeout ..... 2 - 68
2.13.12 lacp actor admin state passive ..... 2 - 69
2.13.13 lacp actor port ..... 2 - 69
2.13.14 lacp actor port priority ..... 2 - 69
2.13.15 lacp actor system priority ..... 2 - 70
2.13.16 lacp partner admin key ..... 2 - 70
2.13.17 lacp partner admin state ..... 2 - 71
2.13.18 lacp partner admin state individual ..... 2 - 71
2.13.19 lacp partner admin state longtimeout ..... 2 - 71
2.13.20 lacp partner admin state passive ..... 2 - 72
2.13.21 lacp partner port id ..... 2 - 72
2.13.22 lacp partner port priority ..... 2 - 73
2.13.23 lacp partner system-id ..... 2 - 73
2.13.24 lacp partner system priority ..... 2 - 73

2.13.25 port-channel static ....2 - 74
2.13.26 port lacpmode ....2 - 74
2.13.27 port lacpmode all ....2 - 74
2.13.28 port lacptimeout (Interface Config) ....2 - 75
2.13.29 port lacptimeout (Global Config) ....2 - 75
2.13.30 port-channel adminmode ....2 - 75
2.13.31 port-channel linktrap ....2 - 76
2.13.32 port-channel load-balance ....2 - 76
2.13.33 port-channel hash multicast ....2 - 77
2.13.34 port-channel name ....2 - 77
2.13.35 port-channel system priority ....2 - 77
2.13.36 show lacp actor ....2 - 78
2.13.37 show lacp partner ....2 - 78
2.13.38 show port-channel brief ....2 - 78
2.13.39 show port-channel ....2 - 79
2.13.40 show port-channel system priority ....2 - 79
2.13.41 show port-channel hash multicast ....2 - 79
2.14 Port Mirroring ....2 - 80
2.14.1 monitor session ....2 - 80
2.14.2 no monitor ....2 - 80
2.14.3 show monitor session ....2 - 81
2.15 Static MAC Filtering ....2 - 81
2.15.1 macfilter ....2 - 81
2.15.2 macfilter adddest ....2 - 82
2.15.3 macfilter adddest all ....2 - 82
2.15.4 macfilter addsrc ....2 - 83
2.15.5 macfilter addsrc all ....2 - 83
2.15.6 show mac-address-table static ....2 - 84
2.15.7 show mac-address-table staticfiltering ....2 - 84
2.16 DHCP L2 Relay Agent Commands ....2 - 84
2.16.1 dhcp l2relay ....2 - 84
2.16.2 dhcp l2relay circuit-id subscription-name ....2 - 85
2.16.3 dhcp l2relay circuit-id vlan ....2 - 85
2.16.4 dhcp l2relay remote-id subscription-name ....2 - 86
2.16.5 dhcp l2relay remote-id vlan ....2 - 86
2.16.6 dhcp l2relay subscription-name ....2 - 86
2.16.7 dhcp l2relay trust ....2 - 87
2.16.8 dhcp l2relay vlan ....2 - 87
2.16.9 show dhcp l2relay all ....2 - 88
2.16.10 show dhcp l2relay interface ....2 - 88
2.16.11 show dhcp l2relay stats interface ....2 - 88
2.16.12 show dhcp l2relay subscription interface ....2 - 89
2.16.13 show dhcp l2relay agent-option vlan ....2 - 89
2.17 DHCP Client Commands ....2 - 90
2.17.1 dhcp client vendor-id-option ....2 - 90

2.17.2 dhcp client vendor-id-option-string ..... 2 - 90
2.17.3 show dhcp client vendor-id-option ..... 2 - 90
2.17.4 ip dhcp force-client-id ..... 2 - 91
2.17.5 show ip dhcp force-client-id ..... 2 - 91
2.17.6 clear ip dhcp force-client-id ..... 2 - 91
2.18 Dynamic ARP Inspection Commands ..... 2 - 91
2.18.1 ip arp inspection vlan ..... 2 - 92
2.18.2 ip arp inspection validate ..... 2 - 92
2.18.3 ip arp inspection vlan logging ..... 2 - 92
2.18.4 ip arp inspection trust ..... 2 - 93
2.18.5 ip arp inspection limit ..... 2 - 93
2.18.6 ip arp inspection filter ..... 2 - 93
2.18.7 arp access-list ..... 2 - 94
2.18.8 permit ip host mac host ..... 2 - 94
2.18.9 show ip arp inspection ..... 2 - 94
2.18.10 show ip arp inspection statistics ..... 2 - 95
2.18.11 clear ip arp inspection statistics ..... 2 - 96
2.18.12 show ip arp inspection interfaces ..... 2 - 96
2.18.13 show arp access-list ..... 2 - 97
2.19 IGMP Snooping Configuration Commands ..... 2 - 97
2.19.1 set igmp ..... 2 - 97
2.19.2 set igmp interfacemode ..... 2 - 98
2.19.3 set igmp fast-leave ..... 2 - 98
2.19.4 set igmp groupmembership-interval ..... 2 - 99
2.19.5 set igmp maxresponse ..... 2 - 100
2.19.6 set igmp mcrtrexpiretime ..... 2 - 100
2.19.7 set igmp mrouter ..... 2 - 101
2.19.8 set igmp mrouter interface ..... 2 - 101
2.19.9 show igmpsnooping ..... 2 - 101
2.19.10 show igmpsnooping mrouter interface ..... 2 - 102
2.19.11 show igmpsnooping mrouter vlan ..... 2 - 103
2.19.12 show igmpsnooping proxy-report ..... 2 - 103
2.19.13 show mac-address-table igmpsnooping ..... 2 - 103
2.20 IGMP Snooping Querier Commands ..... 2 - 103
2.20.1 set igmp querier ..... 2 - 104
2.20.2 set igmp querier query-interval ..... 2 - 104
2.20.3 set igmp querier timer expiry ..... 2 - 105
2.20.4 set igmp querier version ..... 2 - 105
2.20.5 set igmp querier election participate ..... 2 - 105
2.20.6 show igmpsnooping querier ..... 2 - 106
2.21 MLD Snooping Commands ..... 2 - 106
2.21.1 set mld ..... 2 - 107
2.21.2 set mld interfacemode ..... 2 - 107
2.21.3 set mld fast-leave ..... 2 - 108
2.21.4 set mld groupmembership-interval ..... 2 - 108

2.21.5 set mld maxresponse ....2 - 109
2.21.6 set mld mcrtexpiretime ....2 - 109
2.21.7 set mld mrouter ....2 - 109
2.21.8 set mld mrouter interface ....2 - 110
2.21.9 show mldsnooping ....2 - 110
2.21.10 show mldsnooping mrouter interface ....2 - 111
2.21.11 show mldsnooping mrouter vlan ....2 - 111
2.21.12 show mac-address-table mldsnooping ....2 - 111
2.22 MLD Snooping Querier Commands ....2 - 112
2.22.1 set mld querier ....2 - 112
2.22.2 set mld querier query_interval ....2 - 112
2.22.3 set mld querier timer expiry ....2 - 113
2.22.4 set mld querier election participate ....2 - 113
2.22.5 show mldsnooping querier ....2 - 114
2.23 Port Security Commands ....2 - 115
2.23.1 port-security ....2 - 115
2.23.2 port-security max-dynamic ....2 - 115
2.23.3 port-security max-static ....2 - 115
2.23.4 port-security mac-address ....2 - 116
2.23.5 port-security mac-address move ....2 - 116
2.23.6 show port-security ....2 - 116
2.23.7 show port-security dynamic ....2 - 117
2.23.8 show port-security static ....2 - 117
2.23.9 show port-security violation ....2 - 117
2.24 LLDP (802.1AB) Commands ....2 - 117
2.24.1 lldp transmit ....2 - 117
2.24.2 lldp receive ....2 - 118
2.24.3 lldp timers ....2 - 118
2.24.4 lldp transmit-tlv ....2 - 118
2.24.5 lldp transmit-mgmt ....2 - 119
2.24.6 lldp notification ....2 - 119
2.24.7 lldp notification-interval ....2 - 120
2.24.8 clear lldp statistics ....2 - 120
2.24.9 clear lldp remote-data ....2 - 120
2.24.10 show lldp ....2 - 120
2.24.11 show lldp interface ....2 - 121
2.24.12 show lldp statistics ....2 - 121
2.24.13 show lldp remote-device ....2 - 122
2.24.14 show lldp remote-device detail ....2 - 122
2.24.15 show lldp local-device ....2 - 123
2.24.16 show lldp local-device detail ....2 - 124
2.25 LLDP-MED Commands ....2 - 124
2.25.1 lldp med ....2 - 124
2.25.2 lldp med confignotification ....2 - 125
2.25.3 lldp med transmit-tlv ....2 - 125

2.25.4 lldp med all ..... 2 - 125
2.25.5 lldp med confignotification all ..... 2 - 126
2.25.6 lldp med faststartrepeatcount ..... 2 - 126
2.25.7 lldp med transmit-tlv all ..... 2 - 126
2.25.8 show lldp med ..... 2 - 127
2.25.9 show lldp med interface ..... 2 - 127
2.25.10 show lldp med local-device detail ..... 2 - 128
2.25.11 show lldp med remote-device ..... 2 - 129
2.25.12 show lldp med remote-device detail ..... 2 - 129
2.26 Denial of Service Commands ..... 2 - 130
2.26.1 dos-control all ..... 2 - 131
2.26.2 dos-control sipdip ..... 2 - 131
2.26.3 dos-control firstfrag ..... 2 - 132
2.26.4 dos-control tcpfrag ..... 2 - 132
2.26.5 dos-control tcpflag ..... 2 - 132
2.26.6 dos-control l4port ..... 2 - 133
2.26.7 dos-control icmp ..... 2 - 133
2.26.8 dos-control smacdmac ..... 2 - 134
2.26.9 dos-control tcpport ..... 2 - 134
2.26.10 dos-control udpport ..... 2 - 135
2.26.11 dos-control tcpflagseq ..... 2 - 135
2.26.12 dos-control tcpoffset ..... 2 - 135
2.26.13 dos-control tcpsyn ..... 2 - 136
2.26.14 dos-control tcpsynfin ..... 2 - 136
2.26.15 dos-control tcpfinurgpsh ..... 2 - 137
2.26.16 dos-control icmpv4 ..... 2 - 137
2.26.17 dos-control icmpv6 ..... 2 - 138
2.26.18 dos-control icmpfrag ..... 2 - 138
2.26.19 show dos-control ..... 2 - 138
2.27 MAC Database Commands ..... 2 - 139
2.27.1 bridge aging-time ..... 2 - 139
2.27.2 show forwardingdb agetime ..... 2 - 140
2.27.3 show mac-address-table multicast ..... 2 - 140
2.27.4 show mac-address-table stats ..... 2 - 141
2.28 ISDP Commands ..... 2 - 141
2.28.1 isdp run ..... 2 - 141
2.28.2 isdp holdtime ..... 2 - 141
2.28.3 isdp timer ..... 2 - 141
2.28.4 isdp advertise-v2 ..... 2 - 142
2.28.5 isdp enabl ..... 2 - 142
2.28.6 clear isdp counters ..... 2 - 142
2.28.7 clear isdp table ..... 2 - 142
2.28.8 show isdp ..... 2 - 143
2.28.9 show isdp interface ..... 2 - 143
2.28.10 show isdp entry ..... 2 - 143

2.28.11 show isdp neighbors ....2 - 144
2.28.12 show isdp traffic ....2 - 145
2.28.13 debug isdp packet ....2 - 145
2.29 Multicast Handling Commands ....2 - 145
2.29.1 multicast (interface) ....2 - 145
2.29.2 show port multicast ....2 - 146
2.29.3 multicast (VLAN) ....2 - 146
2.29.4 show vlan multicast ....2 - 146
2.29.5 set igmp proxy-report interfacemode ....2 - 146
2.30 Port Bridging Commands ....2 - 147
2.30.1 L2-port-bridge ....2 - 147
2.30.2 show port L2-port-bridge ....2 - 147

Chapter 3

3. Quality of Service Commands ....3 - 2
3.1 Class of Service 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
3.1.12 show protection-group ....3 - 6
3.1.13 protection-group (configure) ....3 - 7
3.1.14 protection-group (interface) ....3 - 7
3.1.15 clear protection-group ....3 - 8
3.2 Differentiated Services Commands ....3 - 8
3.2.1 diffserv ....3 - 9
3.3 DiffServ Class Commands ....3 - 9
3.3.1 class-map ....3 - 9
3.3.2 class-map rename ....3 - 10
3.3.3 match ethertype ....3 - 10
3.3.4 match any ....3 - 10
3.3.5 match class-map ....3 - 11
3.3.6 match cos ....3 - 11
3.3.7 match secondary-cos ....3 - 12
3.3.8 match destination-address mac ....3 - 12

3.3.9 match dstip ..... 3 - 12
3.3.10 match dstip6 ..... 3 - 13
3.3.11 match dstl4port ..... 3 - 13
3.3.12 match ip dscp ..... 3 - 13
3.3.13 match ip precedence ..... 3 - 13
3.3.14 match ip tos ..... 3 - 14
3.3.15 match protocol ..... 3 - 14
3.3.16 match source-address mac ..... 3 - 14
3.3.17 match srcip ..... 3 - 15
3.3.18 match srcip6 ..... 3 - 15
3.3.19 match srcl4port ..... 3 - 15
3.3.20 match vlan ..... 3 - 16
3.3.21 match secondary-vlan ..... 3 - 16
3.4 DiffServ Policy Commands ..... 3 - 16
3.4.1 assign-queue ..... 3 - 17
3.4.2 drop ..... 3 - 17
3.4.3 mirror ..... 3 - 17
3.4.4 redirect ..... 3 - 17
3.4.5 conform-color ..... 3 - 17
3.4.6 class ..... 3 - 18
3.4.7 mark cos ..... 3 - 18
3.4.8 mark cos-as-sec-cos ..... 3 - 19
3.4.9 mark ip-dscp ..... 3 - 19
3.4.10 mark ip-precedence ..... 3 - 19
3.4.11 police-simple ..... 3 - 19
3.4.12 policy-map ..... 3 - 20
3.4.13 policy-map rename ..... 3 - 20
3.5 DiffServ Service Commands ..... 3 - 20
3.5.1 service-policy ..... 3 - 21
3.6 DiffServ Show Commands ..... 3 - 21
3.6.1 show class-map ..... 3 - 22
3.6.2 show diffserv ..... 3 - 22
3.6.3 show policy-map ..... 3 - 23
3.6.4 show diffserv service ..... 3 - 25
3.6.5 show diffserv service brief ..... 3 - 25
3.6.6 show policy-map interface ..... 3 - 26
3.6.7 show service-policy ..... 3 - 26
3.7 MAC Access Control List Commands ..... 3 - 27
3.7.1 mac access-list extended ..... 3 - 27
3.7.2 mac access-list extended rename ..... 3 - 27
3.7.3 {deny | permit} (MAC ACL) ..... 3 - 28
3.7.4 mac access-group ..... 3 - 29
3.7.5 show mac access-lists ..... 3 - 30
3.8 IP Access Control List Commands ..... 3 - 30
3.8.1 access-list ..... 3 - 31

3.8.2 ip access-list ....3 - 32
3.8.3 ip access-list rename ....3 - 32
3.8.4 {deny | permit} (IP ACL) ....3 - 32
3.8.5 ip access-group ....3 - 33
3.8.6 acl-trapflags ....3 - 34
3.8.7 show acl-traptimer ....3 - 34
3.8.8 acl-traptimer ....3 - 34
3.8.9 show ip access-lists ....3 - 35
3.8.10 show access-lists ....3 - 35
3.9 IPv6 Access Control List Commands ....3 - 36
3.9.1 ipv6 access-list ....3 - 36
3.9.2 ipv6 access-list rename ....3 - 36
3.9.3 {deny | permit} (IPv6) ....3 - 37
3.9.4 ipv6 traffic-filter ....3 - 37
3.9.5 show ipv6 access-lists ....3 - 38
3.10 Auto-Voice over IP Commands ....3 - 39
3.10.1 auto-voip all ....3 - 39
3.10.2 auto-voip ....3 - 39
3.10.3 show auto-voip ....3 - 39
3.11 iSCSI Optimization Commands ....3 - 40
3.11.1 iscsi aging time ....3 - 40
3.11.2 iscsi cos ....3 - 40
3.11.3 iscsi enable ....3 - 41
3.11.4 iscsi target port ....3 - 41
3.11.5 show iscsi ....3 - 42
3.11.6 show iscsi sessions ....3 - 43

Chapter 4

4. Routing Commands ....4 - 2
4.1 Address Resolution Protocol Commands ....4 - 2
4.1.1 arp ....4 - 2
4.1.2 ip proxy-arp ....4 - 3
4.1.3 arp cachesize ....4 - 3
4.1.4 arp dynamicrenew ....4 - 3
4.1.5 arp purge ....4 - 4
4.1.6 arp resptime ....4 - 4
4.1.7 arp retries ....4 - 4
4.1.8 arp timeout ....4 - 5
4.1.9 clear arp-cache ....4 - 5
4.1.10 clear arp-switch ....4 - 5
4.1.11 show arp ....4 - 5
4.1.12 show arp brief ....4 - 6

4.1.13 show arp switch ..... 4 - 6
4.2 IP Routing Commands ..... 4 - 7
4.2.1 routing ..... 4 - 7
4.2.2 ip routing ..... 4 - 7
4.2.3 ip address ..... 4 - 7
4.2.4 ip route ..... 4 - 8
4.2.5 ip route default ..... 4 - 9
4.2.6 ip route distance ..... 4 - 9
4.2.7 ip netdirbcast ..... 4 - 9
4.2.8 ip mtu ..... 4 - 10
4.2.9 encapsulation ..... 4 - 10
4.2.10 show ip brief ..... 4 - 11
4.2.11 show ip interface ..... 4 - 11
4.2.12 show ip interface brief ..... 4 - 12
4.2.13 show ip route ..... 4 - 13
4.2.14 show ip route summary ..... 4 - 14
4.2.15 show ip route preferences ..... 4 - 15
4.2.16 show ip stats ..... 4 - 15
4.3 Router Discovery Protocol Commands ..... 4 - 15
4.3.1 ip irdp ..... 4 - 16
4.3.2 ip irdp address ..... 4 - 16
4.3.3 ip irdp holdtime ..... 4 - 16
4.3.4 ip irdp maxadvertinterval ..... 4 - 17
4.3.5 ip irdp minadvertinterval ..... 4 - 17
4.3.6 ip irdp preference ..... 4 - 17
4.3.7 show ip irdp ..... 4 - 18
4.4 Virtual LAN Routing Commands ..... 4 - 18
4.4.1 vlan routing ..... 4 - 18
4.4.2 show ip vlan ..... 4 - 20
4.5 Virtual Router Redundancy Protocol Commands ..... 4 - 20
4.5.1 ip vrrp (Global Config) ..... 4 - 20
4.5.2 ip vrrp (Interface Config) ..... 4 - 21
4.5.3 ip vrrp mode ..... 4 - 21
4.5.4 ip vrrp ip ..... 4 - 21
4.5.5 ip vrrp authentication ..... 4 - 22
4.5.6 ip vrrp preempt ..... 4 - 22
4.5.7 ip vrrp priority ..... 4 - 22
4.5.8 ip vrrp timers advertise ..... 4 - 23
4.5.9 ip vrrp track interface ..... 4 - 23
4.5.10 ip vrrp track ip route ..... 4 - 24
4.5.11 show ip vrrp interface stats ..... 4 - 24
4.5.12 show ip vrrp ..... 4 - 25
4.5.13 show ip vrrp interface ..... 4 - 26
4.5.14 show ip vrrp interface brief ..... 4 - 26
4.6 DHCP and BOOTP Relay Commands ..... 4 - 27

4.6.1 bootpdhcprelay cidoptmode ....4 - 27
4.6.2 bootpdhcprelay maxhopcount ....4 - 27
4.6.3 bootpdhcprelay minwaittime ....4 - 27
4.6.4 show bootpdhcprelay ....4 - 28
4.7 IP Helper Commands ....4 - 28
4.7.1 clear ip helper statistics ....4 - 30
4.7.2 ip helper-address (Global Config) ....4 - 30
4.7.3 ip helper-address (Interface Config) ....4 - 31
4.7.4 ip helper enable ....4 - 33
4.7.5 show ip helper-address ....4 - 33
4.7.6 show ip helper statistics ....4 - 34
4.8 Open Shortest Path First Commands ....4 - 35
4.8.1 router ospf ....4 - 35
4.8.2 enable (OSPF) ....4 - 35
4.8.3 network area (OSPF) ....4 - 35
4.8.4 ip ospf area ....4 - 36
4.8.5 1583compatibility ....4 - 36
4.8.6 area default-cost (OSPF) ....4 - 36
4.8.7 area nssa (OSPF) ....4 - 36
4.8.8 area nssa default-info-originate (OSPF) ....4 - 37
4.8.9 area nssa no-redistribute (OSPF) ....4 - 37
4.8.10 area nssa no-summary (OSPF) ....4 - 37
4.8.11 area nssa translator-role (OSPF) ....4 - 38
4.8.12 area nssa translator-stab-intv (OSPF) ....4 - 38
4.8.13 area range (OSPF) ....4 - 38
4.8.14 area stub (OSPF) ....4 - 39
4.8.15 area stub no-summary (OSPF) ....4 - 39
4.8.16 area virtual-link (OSPF) ....4 - 39
4.8.17 area virtual-link authentication ....4 - 40
4.8.18 area virtual-link dead-interval (OSPF) ....4 - 40
4.8.19 area virtual-link hello-interval (OSPF) ....4 - 41
4.8.20 area virtual-link retransmit-interval (OSPF) ....4 - 41
4.8.21 area virtual-link transmit-delay (OSPF) ....4 - 41
4.8.22 auto-cost (OSPF) ....4 - 42
4.8.23 bandwidth ....4 - 42
4.8.24 capability opaque ....4 - 43
4.8.25 clear ip ospf ....4 - 43
4.8.26 clear ip ospf configuration ....4 - 43
4.8.27 clear ip ospf counters ....4 - 43
4.8.28 clear ip ospf neighbor ....4 - 43
4.8.29 clear ip ospf neighbor interface ....4 - 44
4.8.30 clear ip ospf redistribution ....4 - 44
4.8.31 default-information originate (OSPF) ....4 - 44
4.8.32 default-metric (OSPF) ....4 - 44
4.8.33 distance ospf (OSPF) ....4 - 45
4.8.34 distribute-list out (OSPF) ....4 - 45

4.8.35 exit-overflow-interval (OSPF) ..... 4 - 45
4.8.36 external-lsdb-limit (OSPF) ..... 4 - 46
4.8.37 ip ospf authentication ..... 4 - 46
4.8.38 ip ospf cost ..... 4 - 46
4.8.39 ip ospf dead-interval ..... 4 - 47
4.8.40 ip ospf hello-interval ..... 4 - 47
4.8.41 ip ospf network ..... 4 - 48
4.8.42 ip ospf priority ..... 4 - 48
4.8.43 ip ospf retransmit-interval ..... 4 - 48
4.8.44 ip ospf transmit-delay ..... 4 - 49
4.8.45 ip ospf mtu-ignore ..... 4 - 49
4.8.46 router-id (OSPF) ..... 4 - 49
4.8.47 redistribute (OSPF) ..... 4 - 50
4.8.48 maximum-paths (OSPF) ..... 4 - 50
4.8.49 passive-interface default (OSPF) ..... 4 - 50
4.8.50 passive-interface (OSPF) ..... 4 - 51
4.8.51 timers spf ..... 4 - 51
4.8.52 trapflags (OSPF) ..... 4 - 51
4.8.53 show ip ospf ..... 4 - 53
4.8.54 show ip ospf area ..... 4 - 56
4.8.55 show ip ospf asbr ..... 4 - 57
4.8.56 show ip ospf database ..... 4 - 57
4.8.57 show ip ospf database database-summary ..... 4 - 58
4.8.58 show ip ospf interface ..... 4 - 59
4.8.59 show ip ospf interface brief ..... 4 - 60
4.8.60 show ip ospf interface stats ..... 4 - 61
4.8.61 show ip ospf neighbor ..... 4 - 62
4.8.62 show ip ospf range ..... 4 - 64
4.8.63 show ip ospf statistics ..... 4 - 64
4.8.64 show ip ospf stub table ..... 4 - 65
4.8.65 show ip ospf virtual-link ..... 4 - 65
4.8.66 show ip ospf virtual-link brief ..... 4 - 65
4.9 Routing Information Protocol Commands ..... 4 - 66
4.9.1 router rip ..... 4 - 66
4.9.2 enable (RIP) ..... 4 - 66
4.9.3 ip rip ..... 4 - 66
4.9.4 auto-summary ..... 4 - 67
4.9.5 default-information originate (RIP) ..... 4 - 67
4.9.6 default-metric (RIP) ..... 4 - 67
4.9.7 distance rip ..... 4 - 68
4.9.8 distribute-list out (RIP) ..... 4 - 68
4.9.9 ip rip authentication ..... 4 - 68
4.9.10 ip rip receive version ..... 4 - 69
4.9.11 ip rip send version ..... 4 - 69
4.9.12 hostroutesaccept ..... 4 - 69
4.9.13 split-horizon ..... 4 - 70

4.9.14 redistribute (RIP) ....4 - 70
4.9.15 show ip rip ....4 - 70
4.9.16 show ip rip interface brief ....4 - 71
4.9.17 show ip rip interface ....4 - 71
4.10 ICMP Throttling Commands ....4 - 72
4.10.1 ip unreachables ....4 - 72
4.10.2 ip redirects ....4 - 72
4.10.3 ip icmp echo-reply ....4 - 73
4.10.4 ip icmp error-interval ....4 - 73

Chapter 5

5. IP Multicast Commands ....5 - 2
5.1 Multicast Commands ....5 - 2
5.1.1 ip mcast boundary ....5 - 2
5.1.2 ip multicast ....5 - 2
5.1.3 ip multicast ttl-threshold ....5 - 3
5.1.4 show ip mcast ....5 - 3
5.1.5 show ip mcast boundary ....5 - 4
5.1.6 show ip mcast interface ....5 - 4
5.1.7 show ip mcast mroute ....5 - 4
5.1.8 show ip mcast mroute group ....5 - 5
5.1.9 show ip mcast mroute source ....5 - 5
5.2 DVMRP Commands ....5 - 6
5.2.1 ip dvmrp ....5 - 6
5.2.2 ip dvmrp metric ....5 - 6
5.2.3 ip dvmrp trapflags ....5 - 7
5.2.4 ip dvmrp ....5 - 7
5.2.5 show ip dvmrp ....5 - 7
5.2.6 show ip dvmrp interface ....5 - 8
5.2.7 show ip dvmrp neighbor ....5 - 8
5.2.8 show ip dvmrp nexthop ....5 - 9
5.2.9 show ip dvmrp prune ....5 - 9
5.2.10 show ip dvmrp route ....5 - 9
5.3 PIM-DM Commands ....5 - 10
5.3.1 ip pimdm (Global Config) ....5 - 10
5.3.2 ip pimdm (Interface Config) ....5 - 10
5.3.3 ip pimdm hello-interval ....5 - 11
5.3.4 show ip pimdm ....5 - 11
5.3.5 show ip pimdm interface ....5 - 11
5.3.6 show ip pimdm interface stats ....5 - 12
5.3.7 show ip pimdm neighbor ....5 - 12
5.4 PIM-SM Commands ....5 - 12

5.4.1 ip pimsm ..... 5 - 12
5.4.2 ip pimsm bsr-border ..... 5 - 13
5.4.3 ip pimsm bsr-candidate ..... 5 - 13
5.4.4 ip pimsm dr-priority ..... 5 - 14
5.4.5 ip pimsm hello-interval ..... 5 - 14
5.4.6 ip pimsm join-prune-interval ..... 5 - 14
5.4.7 ip pimsm register-threshold ..... 5 - 15
5.4.8 ip pimsm rp-address ..... 5 - 15
5.4.9 ip pimsm rp-candidate ..... 5 - 15
5.4.10 ip pimsm spt-threshold ..... 5 - 16
5.4.11 ip pimsm ssm ..... 5 - 16
5.4.12 ip pim-trapflags ..... 5 - 16
5.4.13 show ip pimsm ..... 5 - 17
5.4.14 show ip pimsm bsr ..... 5 - 17
5.4.15 show ip pimsm interface ..... 5 - 17
5.4.16 show ip pimsm neighbor ..... 5 - 18
5.4.17 show ip pimsm rphash ..... 5 - 18
5.4.18 show ip pimsm rp mapping ..... 5 - 19
5.5 Internet Group Message Protocol Commands ..... 5 - 19
5.5.1 ip igmp ..... 5 - 19
5.5.2 ip igmp version ..... 5 - 19
5.5.3 ip igmp last-member-query-count ..... 5 - 20
5.5.4 ip igmp last-member-query-interval ..... 5 - 20
5.5.5 ip igmp query-interval ..... 5 - 20
5.5.6 ip igmp query-max-response-time ..... 5 - 21
5.5.7 ip igmp robustness ..... 5 - 21
5.5.8 ip igmp startup-query-count ..... 5 - 21
5.5.9 ip igmp startup-query-interval ..... 5 - 22
5.5.10 show ip igmp ..... 5 - 22
5.5.11 show ip igmp groups ..... 5 - 22
5.5.12 show ip igmp interface ..... 5 - 23
5.5.13 show ip igmp interface membership ..... 5 - 24
5.5.14 show ip igmp interface stats ..... 5 - 25
5.6 IGMP Proxy Commands ..... 5 - 25
5.6.1 ip igmp-proxy ..... 5 - 25
5.6.2 ip igmp-proxy unsolicit-rprt-interval ..... 5 - 25
5.6.3 ip igmp-proxy reset-status ..... 5 - 26
5.6.4 show ip igmp-proxy ..... 5 - 26
5.6.5 show ip igmp-proxy interface ..... 5 - 27
5.6.6 show ip igmp-proxy groups ..... 5 - 27
5.6.7 show ip igmp-proxy groups detail ..... 5 - 28

Chapter 6

6. Utility Commands ....6 - 2
6.1 Dual Image Commands ....6 - 2
6.1.1 delete ....6 - 2
6.1.2 delete nvram:file <file> ....6 - 2
6.1.3 boot system ....6 - 3
6.1.4 show bootvar ....6 - 3
6.2 System Information and Statistics Commands ....6 - 3
6.2.1 show arp switch ....6 - 3
6.2.2 show eventlog ....6 - 3
6.2.3 show hardware ....6 - 4
6.2.4 show version ....6 - 4
6.2.5 show interface ....6 - 5
6.2.6 show interface ethernet ....6 - 5
6.2.7 show mac-addr-table ....6 - 11
6.2.8 show process cpu ....6 - 12
6.2.9 show running-config ....6 - 13
6.2.10 show sysinfo ....6 - 14
6.2.11 show tech-support ....6 - 14
6.2.12 terminal length ....6 - 14
6.2.13 show terminal length ....6 - 15
6.3 Logging Commands ....6 - 15
6.3.1 logging buffered ....6 - 15
6.3.2 logging buffered wrap ....6 - 15
6.3.3 logging cli-command ....6 - 16
6.3.4 logging console ....6 - 16
6.3.5 logging host ....6 - 16
6.3.6 logging host remove ....6 - 17
6.3.7 logging port ....6 - 17
6.3.8 logging syslog ....6 - 17
6.3.9 show logging ....6 - 18
6.3.10 show logging buffered ....6 - 18
6.3.11 show logging hosts ....6 - 18
6.3.12 show logging traplogs ....6 - 19
6.3.13 show nvram:file ....6 - 19
6.4 System Utility and Clear Commands ....6 - 19
6.4.1 traceroute ....6 - 20
6.4.2 traceroute ipv6 ....6 - 21
6.4.3 clear config ....6 - 21
6.4.4 clear counters ....6 - 21
6.4.5 clear igmpsnooping ....6 - 21

6.4.6 clear pass ..... 6 - 22
6.4.7 clear port-channel ..... 6 - 22
6.4.8 clear traplog ..... 6 - 22
6.4.9 clear vlan ..... 6 - 22
6.4.10 enable passwd ..... 6 - 22
6.4.11 enable passwd encrypted <password> ..... 6 - 22
6.4.12 enable password ..... 6 - 22
6.4.13 logout ..... 6 - 23
6.4.14 ping ..... 6 - 23
6.4.15 quit ..... 6 - 24
6.4.16 reload ..... 6 - 25
6.4.17 set board sensor threshold ..... 6 - 25
6.4.18 reload fast ..... 6 - 25
6.4.19 copy ..... 6 - 25
6.4.20 copy ipmi-hpm ..... 6 - 27
6.4.21 set bootstopkey ..... 6 - 27
6.4.22 show watchdog ..... 6 - 27
6.4.23 set watchdog ..... 6 - 28
6.4.24 show boardinfo post-status ..... 6 - 28
6.4.25 show boardinfo sensors ..... 6 - 28
6.4.26 show boardinfo event-log ..... 6 - 28
6.4.27 show boardinfo update-status ..... 6 - 28
6.4.28 show boardinfo version ..... 6 - 29
6.4.29 show boardinfo address ..... 6 - 29
6.4.30 show boardinfo fru ..... 6 - 29
6.4.31 show boardinfo ipmidev ..... 6 - 30
6.4.32 set board time ..... 6 - 30
6.4.33 show boardinfo time ..... 6 - 30
6.4.34 show boardinfo memory-usage ..... 6 - 30
6.4.35 show boardinfo cpu-load ..... 6 - 30
6.4.36 set board root-password ..... 6 - 30
6.4.37 set board snmp ipmi-trap ..... 6 - 31
6.4.38 set board snmp filter ..... 6 - 31
6.4.39 enable (filter) ..... 6 - 31
6.4.40 disable (filter) ..... 6 - 31
6.4.41 ipmb (filter) ..... 6 - 31
6.4.42 type (filter) ..... 6 - 32
6.4.43 status (filter) ..... 6 - 32
6.4.44 assert (filter) ..... 6 - 32
6.4.45 show boardinfo snmp ipmi-trap ..... 6 - 32
6.5 Commands to configure startup services ..... 6 - 32
6.5.1 set chkconfig ..... 6 - 32
6.5.2 show chkconfig ..... 6 - 33
6.6 Commands supporting SFP/SFP+ (AM4910 only) ..... 6 - 33
6.6.1 show sfp (AM4910 only) ..... 6 - 33
6.6.2 sfp mode (AM4910 only) ..... 6 - 34

6.7 Simple Network Time Protocol Commands ..... 6 - 34
6.7.1 sntp broadcast client poll-interval ..... 6 - 34
6.7.2 sntp client mode ..... 6 - 35
6.7.3 sntp client port ..... 6 - 35
6.7.4 sntp unicast client poll-interval ..... 6 - 36
6.7.5 sntp unicast client poll-timeout ..... 6 - 36
6.7.6 sntp unicast client poll-retry ..... 6 - 36
6.7.7 sntp multicast client poll-interval ..... 6 - 37
6.7.8 sntp server ..... 6 - 37
6.7.9 show sntp ..... 6 - 37
6.7.10 show sntp client ..... 6 - 38
6.7.11 show sntp server ..... 6 - 38
6.7.12 clear board event-log ..... 6 - 39
6.7.13 show logging errcounter ..... 6 - 39
6.7.14 clear errcounter ..... 6 - 39
6.7.15 show logging backtrace ..... 6 - 39
6.8 DHCP Server Commands ..... 6 - 39
6.8.1 ip dhcp pool ..... 6 - 39
6.8.2 client-identifier ..... 6 - 40
6.8.3 client-name ..... 6 - 40
6.8.4 default-router ..... 6 - 40
6.8.5 dns-server ..... 6 - 41
6.8.6 hardware-address ..... 6 - 41
6.8.7 host ..... 6 - 41
6.8.8 lease ..... 6 - 42
6.8.9 network (DHCP Pool Config) ..... 6 - 42
6.8.10 bootfile ..... 6 - 42
6.8.11 domain-name ..... 6 - 43
6.8.12 netbios-name-server ..... 6 - 43
6.8.13 netbios-node-type ..... 6 - 43
6.8.14 next-server ..... 6 - 44
6.8.15 option ..... 6 - 44
6.8.16 ip dhcp excluded-address ..... 6 - 45
6.8.17 ip dhcp ping packets ..... 6 - 45
6.8.18 service dhcp ..... 6 - 45
6.8.19 ip dhcp bootp automatic ..... 6 - 46
6.8.20 ip dhcp conflict logging ..... 6 - 46
6.8.21 clear ip dhcp binding ..... 6 - 46
6.8.22 clear ip dhcp server statistics ..... 6 - 46
6.8.23 clear ip dhcp conflict ..... 6 - 47
6.8.24 show ip dhcp binding ..... 6 - 47
6.8.25 show ip dhcp global configuration ..... 6 - 47
6.8.26 show ip dhcp pool configuration ..... 6 - 47
6.8.27 show ip dhcp server statistics ..... 6 - 48
6.8.28 show ip dhcp conflict ..... 6 - 49
6.9 DNS Client Commands ..... 6 - 49

6.9.1 ip domain lookup ..... 6 - 49
6.9.2 ip domain name ..... 6 - 49
6.9.3 ip domain list ..... 6 - 50
6.9.4 ip name server ..... 6 - 50
6.9.5 ip host ..... 6 - 51
6.9.6 ip domain retry ..... 6 - 51
6.9.7 ip domain timeout ..... 6 - 51
6.9.8 clear host ..... 6 - 52
6.9.9 show hosts ..... 6 - 52
6.10 Serviceability Packet Tracing Commands ..... 6 - 53
6.10.1 debug arp ..... 6 - 53
6.10.2 debug auto-voip ..... 6 - 53
6.10.3 debug clear ..... 6 - 53
6.10.4 debug console ..... 6 - 54
6.10.5 debug dot1x packet ..... 6 - 54
6.10.6 debug igmpsnooping packet ..... 6 - 54
6.10.7 debug igmpsnooping packet transmit ..... 6 - 55
6.10.8 debug igmpsnooping packet receive ..... 6 - 55
6.10.9 debug lacp packet ..... 6 - 56
6.10.10 debug ping packet ..... 6 - 57
6.10.11 debug spanning-tree bpdu ..... 6 - 57
6.10.12 debug spanning-tree bpdu receive ..... 6 - 58
6.10.13 debug spanning-tree bpdu transmit ..... 6 - 58
6.10.14 logging persistent ..... 6 - 59
6.11 Cable Test Command ..... 6 - 59
6.11.1 cablestatus ..... 6 - 60
6.12 sFlow Commands ..... 6 - 60
6.12.1 sflow receiver ..... 6 - 60
6.12.2 sflow sampler ..... 6 - 60
6.12.3 sflow poller ..... 6 - 61
6.12.4 show sflow agent ..... 6 - 61
6.12.5 show sflow receivers ..... 6 - 61
6.12.6 show sflow samplers ..... 6 - 61
6.13 AutoInstall Commands ..... 6 - 62
6.13.1 boot autoinstall ..... 6 - 62
6.13.2 boot autoinstall auto-save ..... 6 - 62
6.13.3 boot autoinstall retry-count ..... 6 - 62
6.13.4 show autoinstall ..... 6 - 62

Chapter 7

7. Management Commands ..... 7 - 2
7.1 Network Interface Commands ..... 7 - 2

7.1.1 enable (Privileged EXEC access) ....7 - 2
7.1.2 clicm ....7 - 2
7.1.3 serviceport ip ....7 - 3
7.1.4 serviceport protocol ....7 - 3
7.1.5 network parms ....7 - 3
7.1.6 network protocol ....7 - 3
7.1.7 network mac-address ....7 - 3
7.1.8 network mac-type ....7 - 4
7.1.9 show network ....7 - 4
7.1.10 show serviceport ....7 - 5
7.2 Console Port Access Commands ....7 - 6
7.2.1 configuration ....7 - 6
7.2.2 line ....7 - 6
7.2.3 serial baudrate ....7 - 6
7.2.4 serial timeout ....7 - 7
7.2.5 show serial ....7 - 7
7.3 Telnet Commands ....7 - 7
7.3.1 ip telnet server enable ....7 - 7
7.3.2 telnet ....7 - 8
7.3.3 telnetcon maxsessions ....7 - 8
7.3.4 telnetcon timeout ....7 - 8
7.3.5 show telnetcon ....7 - 9
7.4 Secure Shell Commands ....7 - 9
7.4.1 ip ssh ....7 - 9
7.4.2 ip ssh protocol ....7 - 10
7.4.3 ip ssh server enable ....7 - 10
7.4.4 sshcon maxsessions ....7 - 10
7.4.5 sshcon timeout ....7 - 10
7.4.6 show ip ssh ....7 - 11
7.5 Management Security Commands ....7 - 11
7.5.1 crypto certificate generate ....7 - 11
7.5.2 crypto key generate rsa ....7 - 12
7.5.3 crypto key generate dsa ....7 - 12
7.6 Hypertext Transfer Protocol Commands ....7 - 12
7.6.1 ip http authentication ....7 - 12
7.6.2 ip https authentication ....7 - 13
7.6.3 ip http server ....7 - 14
7.6.4 ip http secure-server ....7 - 14
7.6.5 ip http java ....7 - 14
7.6.6 ip http session hard-timeout ....7 - 15
7.6.7 ip http session maxsessions ....7 - 15
7.6.8 ip http session soft-timeout ....7 - 15
7.6.9 ip http secure-session hard-timeout ....7 - 16
7.6.10 ip http secure-session maxsessions ....7 - 16
7.6.11 ip http secure-session soft-timeout ....7 - 16

7.6.12 ip http secure-port ..... 7 - 17
7.6.13 ip http secure-protocol ..... 7 - 17
7.6.14 show ip http ..... 7 - 17
7.7 Access Commands ..... 7 - 18
7.7.1 disconnect ..... 7 - 18
7.7.2 show loginsession ..... 7 - 18
7.8 User Account Commands ..... 7 - 18
7.8.1 aaa authentication login ..... 7 - 18
7.8.2 aaa authentication enable ..... 7 - 19
7.8.3 enable authentication ..... 7 - 20
7.8.4 username ..... 7 - 21
7.8.5 username name nopassword ..... 7 - 21
7.8.6 username snmpv3 accessmode ..... 7 - 22
7.8.7 username snmpv3 authentication ..... 7 - 22
7.8.8 username snmpv3 encryption encrypted ..... 7 - 23
7.8.9 show users ..... 7 - 23
7.8.10 show users long ..... 7 - 24
7.8.11 show users accounts ..... 7 - 24
7.8.12 show users login-history ..... 7 - 24
7.8.13 login authentication ..... 7 - 25
7.8.14 passwd ..... 7 - 25
7.8.15 password (Line Configuration) ..... 7 - 25
7.8.16 password (User EXEC) ..... 7 - 26
7.8.17 passwords min-length ..... 7 - 26
7.8.18 passwords history ..... 7 - 26
7.8.19 passwords aging ..... 7 - 27
7.8.20 passwords lock-out ..... 7 - 27
7.8.21 show passwords configuration ..... 7 - 27
7.8.22 write memory ..... 7 - 28
7.9 SNMP Commands ..... 7 - 28
7.9.1 snmp-server ..... 7 - 28
7.9.2 snmp-server community ..... 7 - 28
7.9.3 snmp-server community ipaddr ..... 7 - 29
7.9.4 snmp-server community ipmask ..... 7 - 29
7.9.5 snmp-server community mode ..... 7 - 30
7.9.6 snmp-server community ro ..... 7 - 30
7.9.7 snmp-server enable traps violation ..... 7 - 30
7.9.8 snmp-server enable traps ..... 7 - 31
7.9.9 snmp-server enable traps all ..... 7 - 31
7.9.10 snmp-server enable traps linkmode ..... 7 - 31
7.9.11 snmp-server enable traps multiusers ..... 7 - 32
7.9.12 snmp-server enable traps stpmode ..... 7 - 32
7.9.13 snmptrap ..... 7 - 32
7.9.14 snmptrap snmpversion ..... 7 - 33
7.9.15 snmptrap ipaddr ..... 7 - 33

7.9.16 snmptrap mode ....7 - 33
7.9.17 snmp trap link-status ....7 - 34
7.9.18 snmp trap link-status all ....7 - 34
7.9.19 show snmpcommunity ....7 - 35
7.9.20 show snmptrap ....7 - 35
7.9.21 show trapflags ....7 - 36
7.9.22 snmptrap ....7 - 36
7.9.23 snmptrap notification ....7 - 37
7.9.24 snmp-server engine-id ....7 - 37
7.9.25 show snmp-engine-id ....7 - 38
7.9.26 set board snmp site ....7 - 38
7.9.27 set board snmp sel-clear ....7 - 38
7.9.28 set board snmp interval ....7 - 38
7.9.29 show boardinfo snmp site ....7 - 39
7.9.30 show boardinfo snmp interval ....7 - 39
7.9.31 set board snmp trap ....7 - 39
7.9.32 show boardinfo snmp trap ....7 - 39
7.10 RADIUS Commands ....7 - 39
7.10.1 authorization network radius ....7 - 40
7.10.2 radius accounting mode ....7 - 40
7.10.3 radius server attribute ....7 - 40
7.10.4 radius server host ....7 - 41
7.10.5 radius server key ....7 - 42
7.10.6 radius server msgauth ....7 - 43
7.10.7 radius server primary ....7 - 43
7.10.8 radius server retransmit ....7 - 43
7.10.9 radius server timeout ....7 - 44
7.10.10 show radius ....7 - 44
7.10.11 show radius servers ....7 - 45
7.10.12 show radius accounting ....7 - 46
7.10.13 show radius accounting statistics ....7 - 47
7.10.14 show radius statistics ....7 - 49
7.11 TACACS+ Commands ....7 - 50
7.11.1 tacacs-server host ....7 - 50
7.11.2 tacacs-server key ....7 - 51
7.11.3 tacacs-server timeout ....7 - 51
7.11.4 key ....7 - 51
7.11.5 port ....7 - 52
7.11.6 priority ....7 - 52
7.11.7 timeout ....7 - 52
7.11.8 show tacacs ....7 - 52
7.12 Configuration Scripting Commands ....7 - 53
7.12.1 script apply ....7 - 53
7.12.2 script delete ....7 - 54
7.12.3 script list ....7 - 54

7.12.4 script show ..... 7 - 54
7.12.5 script validate ..... 7 - 54
7.13 Pre-login Banner and System Prompt Commands ..... 7 - 54
7.13.1 copy (pre-login banner) ..... 7 - 55
7.13.2 set prompt ..... 7 - 55

Appendix A

A. List of Commands ..... A - 2

Appendix B

B. FASTPATH Log Messages ..... B - 2
B.1 Core ..... B - 2
B.2 Utilities ..... B - 3
B.3 Management ..... B - 5
B.4 Switching ..... B - 7
B.5 QoS ..... B - 12
B.6 Technologies ..... B - 13
B.7 O/S Support ..... B - 14

Appendix C

C. Getting Help ..... C - 2

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 switch management application. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

To switch from the switching management application CLI to the Carrier Manager CLI, use the command “clicm”, see 7.1.2 “clicm” on page 7 - 2

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 - 3
- 1.3 “Common Parameter Values” on page 1 - 3
- 1.4 “Slot/Port Naming Convention” on page 1 - 4
- 1.5 “Using the “No” Form of a Command” on page 1 - 4
- 1.6 “FASTPATH Modules” on page 1 - 5
- 1.7 “Command Modes” on page 1 - 5
- 1.8 “Command Completion and Abbreviation” on page 1 - 7
- 1.9 “CLI Error Messages” on page 1 - 7
- 1.10 “CLI Line-Editing Conventions” on page 1 - 7
- 1.11 “Using CLI Help” on page 1 - 8
- 1.12 “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 Command 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 1 describes the conventions this document uses to distinguish between value types.

Table 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.

1.3 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 2 describes common parameter values and value formatting.

Table 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)**
ipv6-address	**FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or** **FE80:0:0:0:20F:24FF:FEBF:DBCB, or** **FE80::20F24FF:FEBF:DBCB, or** **FE80:0:0:0:20F:24FF:128:141:49:32** For additional information, refer to RFC 3513.
Interface or slot/port	Valid slot and port number separated by a forward slash. 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.

Table 2: Parameter Descriptions (Continued)

Parameter	Description
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

1.4 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 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: 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.

1.5 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.

1.6 FASTPATH Modules

FASTPATH software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The commands and command modes available on your switch depend on the installed modules. Additionally, for some **show** commands, the output fields might change based on the modules included in the FASTPATH software.

The FASTPATH software suite includes the following modules:

- Switching (Layer 2)
- Quality of Service
- Management (CLI and SNMP)

Not all modules are available for all platforms or software releases.

1.7 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 5 describes the command modes and the prompts visible in that mode.

Note: The command modes available on your switch depend on the software modules that are installed.

Table 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>)#`
		Manages 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.

Line Config	`Switch (line)#`	Contains commands to configure outbound telnet settings and console interface settings.
Policy Map Config	`Switch (Config-policy-map)#`	Contains the QoS Policy-Map configuration commands.

Table 5: CLI Command Modes (Continued)

Command Mode	*Prompt*	*Mode Description*
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)#**	Contains the QoS class map configuration commands for IPv4.
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)#**	Contains commands to configure properties for the TACACS servers.
DHCP Pool Config	**Switch (Config dhcp-pool)#**	Contains the DHCP server IP address pool configuration commands.

Table 6 explains how to enter or exit each mode.

Table 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**.
Interface Config	From the Global Config mode, enter **interface** *<slot/port>* or **interface loopback** *<id>* or **interface tunnel** *<id>*	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**, and specify the optional keyword *ipv4* to specify the Layer 3 protocol for this class. See 3.3.1 “class-map” on page 3 - 9 for more information.	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**.

Table 6: CLI Mode Access and Exit (Continued)

Command Mode	*Access Method*	*Exit or Access Previous Mode*
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**.

1.8 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.

1.9 CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 7 describes the most common CLI error messages.

Table 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.

1.10 CLI Line-Editing Conventions

Table 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 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

Table 8: CLI Editing Conventions (Continued)

Key Sequence	*Description*
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

1.11 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
```

1.12 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 7.1 “Network Interface Commands” on page 7 - 2.

Chapter 2

Switching Commands

2. Switching Commands

This chapter describes the switching commands available in the FASTPATH CLI.

The Switching Commands chapter includes the following sections:

- 2.1 “Port Configuration Commands” on page 2 - 3
- 2.2 “Spanning Tree Protocol (STP) Commands” on page 2 - 7
- 2.3 “VLAN Commands” on page 2 - 20
- 2.4 “Double VLAN Commands” on page 2 - 30
- 2.5 “Voice VLAN Commands” on page 2 - 33
- 2.6 “Provisioning (IEEE 802.1p) Commands” on page 2 - 36
- 2.7 “Protected Ports Commands” on page 2 - 37
- 2.8 “GARP Commands” on page 2 - 39
- 2.9 “GVRP Commands” on page 2 - 40
- 2.10 “GMRP Commands” on page 2 - 42
- 2.11 “Port-Based Network Access Control Commands” on page 2 - 44
- 2.12 “Storm-Control Commands” on page 2 - 55
- 2.13 “Port-Channel/LAG (802.3ad) Commands” on page 2 - 65
- 2.14 “Port Mirroring” on page 2 - 80
- 2.15 “Static MAC Filtering” on page 2 - 81
- 2.16 “DHCP L2 Relay Agent Commands” on page 2 - 84
- 2.17 “DHCP Client Commands” on page 2 - 90
- 2.18 “Dynamic ARP Inspection Commands” on page 2 - 91
- 2.19 “IGMP Snooping Configuration Commands” on page 2 - 97
- 2.20 “IGMP Snooping Querier Commands” on page 2 - 103
- 2.21 “MLD Snooping Commands” on page 2 - 106
- 2.22 “MLD Snooping Querier Commands” on page 2 - 112
- 2.23 “Port Security Commands” on page 2 - 115
- 2.24 “LLDP (802.1AB) Commands” on page 2 - 117
- 2.25 “LLDP-MED Commands” on page 2 - 124
- 2.26 “Denial of Service Commands” on page 2 - 130
- 2.27 “MAC Database Commands” on page 2 - 139
- 2.28 “ISDP Commands” on page 2 - 141
- 2.29 “Multicast Handling Commands” on page 2 - 145
- 2.30 “Port Bridging Commands” on page 2 - 147

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 advertise speed

This command sets auto-negotiation advertised speed parameters. If full/half-duplex is not specified the speed is valid for both modes.

Format **advertise speed** *<1000 | 100 | 10> [<half-duplex | full-duplex>]*

Mode Interface Config

2.1.4.1 no advertise speed

This command resets auto-negotiation advertised speed parameters.

Format **no advertise speed** *<1000 | 100 | 10> [<half-duplex | full-duplex>]*

Mode Interface Config

2.1.5 show advertise speed

This command lists the auto-negotiation advertised speed parameters. The values are listed for a specified interface.

Format **show advertise speed** *<slot/port>*

Mode Privileged Exec

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

Format **block**

Mode Interface Config

2.1.6.1 no block

This command resets a port in non-blocking mode.

Format **no block**

Mode Interface Config

2.1.7 description

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

Format **description** *<description>*

Mode Interface Config

2.1.8 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

2.1.8.1 no mtu

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

Format **no mtu**
Mode Interface Config

2.1.9 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

2.1.9.1 no shutdown

This command enables a port.

Format **no shutdown**
Mode Interface Config

2.1.10 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

2.1.10.1 no shutdown all

This command enables all ports.

Format `no shutdown all`
Mode Global Config

2.1.11 speed

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

Format `speed {<100 | 10> <half-duplex | full-duplex>}`
`speed <1000 | 10000> [full-duplex]`
Mode Interface Config

Acceptable Values	*Definition*
10000	10Gb full-duplex
10000	10Gb
1000	1Gb full-duplex
1000	1Gb
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

2.1.12 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	*Definition*
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

2.1.13 show port

This command displays port information.

Format `show port {<slot/port> | all}`
Mode Privileged EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
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 2.14 “Port Mirroring” on page 2 - 80. • **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.

2.1.14 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

Term	*Definition*
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 bpdufilter

Use this command to enable BPDU Filter on the interface.

Default disabled
Format `spanning-tree bpdufilter`
Mode Interface Config

2.2.2.1 no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface.

Default disabled
Format `no spanning-tree bpdufilter`
Mode Interface Config

2.2.3 spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default disabled
Format **`spanning-tree bpdufilter`**
Mode Global Config

2.2.3.1 no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default disabled
Format **`no spanning-tree bpdufilter default`**
Mode Global Config

2.2.4 spanning-tree bpduflood

Use this command to enable BPDU Flood on the interface.

Default disabled
Format **spanning-tree bpduflood**
Mode Interface Config

2.2.4.1 no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface.

Default disabled
Format **no spanning-tree bpduflood**
Mode Interface Config

2.2.5 spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default disabled
Format **spanning-tree bpduguard**
Mode Global Config

2.2.5.1 no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default disabled
Format **no spanning-tree bpduguard**
Mode Global Config

2.2.6 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

2.2.7 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

2.2.7.1 no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format `no spanning-tree configuration name`
Mode Global Config

2.2.8 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

2.2.8.1 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

2.2.9 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

2.2.9.1 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

2.2.10 spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default 802.1s
Format `spanning-tree forceversion` *<802.1d | 802.1s | 802.1w>*
Mode Global Config

- Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).

- Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

2.2.10.1 no spanning-tree forceversion

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

Format `no spanning-tree forceversion`
Mode Global Config

2.2.11 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

2.2.11.1 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

2.2.12 spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default none
Format `spanning-tree guard` *{ none | root | loop }*
Mode Interface Config

2.2.12.1 no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format `no spanning-tree guard`
Mode Interface Config

2.2.13 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

2.2.13.1 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

2.2.14 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** *<6-40>*
Mode Global Config

2.2.14.1 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

2.2.15 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

2.2.15.1 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

2.2.16 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 4093, 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

2.2.16.1 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

2.2.17 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

2.2.17.1 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 **no spanning-tree mst priority** *<mstid>*

Mode Global Config

2.2.18 spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are 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 vlan range can be specified as a list or as a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash ("-").

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

Mode Global Config

2.2.18.1 no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

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

Mode Global Config

2.2.19 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

2.2.19.1 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

2.2.20 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

2.2.20.1 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

2.2.21 spanning-tree port-state

This command sets the state of a port used by a MST instance. The command sets the spanning tree state (forward/block) of a port for incoming (ingress) or outgoing (egress) traffic or both for an existing MST instance (1..4093). Default state is forwarding. The state of the port can be seen only via “show running-config”. If the state is blocked, the command is displayed (otherwise not).

Default forwarding
Format `spanning-tree mst <mst-id> port-state ingress <forward | block>`
`spanning-tree mst <mst-id> port-state egress <forward | block>`
`spanning-tree mst <mst-id> port-state both <forward | block>`
Mode Interface Config

2.2.22 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`
Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
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.

2.2.23 show spanning-tree brief

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

Format `show spanning-tree brief`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
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).

2.2.24 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>*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Guard Effect	Enabled or disabled.
Root Guard	Enabled or disabled.
Loop Guard	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for **edge delay** time, to become an edge port and transition to forwarding faster.
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.
RSTP 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.

2.2.25 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

Term	*Definition*
Term	*Definition*
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.
Designated Root	The Identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
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.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.

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.

Term	*Definition*
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.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the 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.

Term	Definition
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 Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

2.2.26 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}*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID	The MST instance associated with this port.
Interface	Valid slot and port number separated by a forward slash.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
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.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

2.2.27 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`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: • Associated FIDs • Associated VLANs	• List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

2.2.28 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`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
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.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
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	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

2.2.29 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>*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
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** *<1-4093>*
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 2-4093.

Format **vlan** *<2-4093>*
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 2-4093.

Format **no vlan** *<2-4093>*
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 2-4093.

Format `vlan makestatic` *<2-4093>*
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 1-4093.

Default
- VLAN ID 1 - default
- other VLANS - blank string

Format `vlan name` *<2-4093> <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` *<2-4093>*

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} <1-4093>*

Mode Interface Config

Participation options are:

Participation Options	*Definition*
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.

Format **vlan participation all** *{exclude | include | auto} <1-4093>*

Mode Global Config

You can use the following participation options:

Participation Options	*Definition*
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.

2.3.10 vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default all

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

Mode Global Config

The modes defined as follows:

Mode	*Definition*
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.

Mode	*Definition*
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.

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` *<1-4093>*

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** *<1-4093>*
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.

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.

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.

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** *<1-4093>*
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** *<1-4093>*
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** *<1-4093>*
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>*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
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 a forward slash. 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.

Term	Definition
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`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
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}*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Valid slot and port number separated by a forward slash. 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.

Term	Definition
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

Term	Definition
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

Term	Definition
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 (Global Config)

This command configures the ethertype for all interfaces. The two-byte hex ethertype is used as the first 16 bits of the DVLAN tag. The ethertype may have the values of *`802.1Q`*, *`vMAN`*, or *`custom`*. If the ethertype has an optional value of *`custom`*, then it is a custom tunnel value, and ethertype must be set to a value in the range of 0 to 65535.

Default vman

Format **dvlan-tunnel ethertype** *{802.1Q | vman | custom <0-65535>}*

Mode Global Config

Parameter	*Description*
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 0 to 65535.
vman	Represents the commonly used value of 0x88A8.

2.4.2 dvlan-tunnel ethertype default-tpid

Use this command to create a new TPID and associate it with the next available TPID register. If no TPID registers are empty, the system returns an error to the user. Specifying the optional keyword [default–tpid] forces the TPID value to be configured as the default TPID at index 0.

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

Mode Global Config

Parameter	*Description*
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 0 to 65535.
vman	Represents the commonly used value of 0x88A8.

2.4.2.1 no dvlan-tunnel ethertype default–tpid

Use the `no` form of the command to set the TPID register to 0. (At initialization, all TPID registers will be set to their default values.)

Format **no dvlan-tunnel ethertype** *{<802.1Q | vman> | custom <0-65535>} [default-tpid]*

Mode Global Config

2.4.3 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

2.4.3.1 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

2.4.4 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

2.4.4.1 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

2.4.5 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}]`*
Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
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.

2.4.6 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}]*

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
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.

Example: The following shows examples of the CLI display output for the commands.

```
(Broadcom FASTPATH Routing) #show dvlan-tunnel

TPIDs Configured.............................. 0x88a8
Default TPID.................................. 0x88a8
Interfaces Enabled for DVLAN Tunneling......... None

(Broadcom FASTPATH Routing) #

(switch)#show dvlan-tunnel interface 1/0/1

Interface Mode    EtherType
--------- ------- ------------
1/0/1     Disable 0x88a8
```

2.5 Voice VLAN Commands

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

2.5.1 voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default disabled

Format `voice vlan`
Mode Global Config

2.5.1.1 no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format `no voice vlan`
Mode Global Config

2.5.2 voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface.

Default disabled
Format `voice vlan {vlanid <id> | dot1p <priority> | none | untagged}`
Mode Interface Config

You can configure Voice VLAN in one of four different ways:

Parameter	*Description*
vlan-id	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4093 (the max supported by the platform).
dot1p	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid *<priority>* range is 0 to 7.
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

2.5.2.1 no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format `no voice vlan`
Mode Interface Config

2.5.3 voice vlan data priority

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN port.

Default trust
Format `voice vlan data priority untrust | trust`
Mode Interface Config

2.5.4 show voice vlan

Format `show voice vlan [interface {<slot/port> | all}]`
Mode Privileged EXEC

When the **interface** parameter is not specified, only the global mode of the Voice VLAN is displayed.

Term	*Definition*
Administrative Mode	The Global Voice VLAN mode.

When the **interface** is specified:

Term	*Definition*
Voice VLAN Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

Parameter	*Description*
service-name	The user-assigned service name.
svid	The service VLAN ID (S-VID).

Parameter	*Description*
e-lan | e-line | e-tree | tls	These parameters define the type of traffic associated with this service instance. • **e-ian** — A switched or general service is one in which the traffic associated with that service is forwarded based on a standard L2 switching lookup using the S-VID and destination MAC as lookups in the FDB. In FASTPATH a port can be a member of multiple E-LAN services. If a switched service is assigned to multiple UNI ports, those ports will be able to forward traffic to each other as well as to the NNI ports. The same E-LAN service can also be applied on UNI-P and UNI-S ports. • **e-line** — The *e-line* parameter creates a point-to-point service, in which traffic is forwarded directly to the NNI port in the upstream direction and to the associated UNI port in the downstream direction. An e-line service bypasses the standard VLAN/MAC-based switching decisions, including the source MAC learing. Be default, FASTPATH does not learn traffic belonging to the e-line service. An e-line service-instance defines a point-to-point service in which only one UNI-P or UNI-S port participates. ***Note:*** It is important to note that downstream broadcast and multicast traffic will still be redirected to the associated UNI port participating in the e-line service. • **e-tree** — The *e-tree* parameter creates a point-to-multipoint service in which the traffic associated with that service is forwarded directly to the NNI port in the upstream direction and direct to the associated UNI port(s) in the downstream direction. If an e-tree service instance is applied to multiple UNI ports, it becomes a point-to-multipoint service in which the participating user ports are still isolated from each other. ***Note:*** It is important to note that downstream broadcast, multicast, and unknown destination (DLF) traffic will still be forwarded (replicated) to all ports participating in the e-tree service. • **tls** (Transparent LAN Service). Administrators can configure a TLS on UNI-P and UNI-S ports. A Transparent LAN service is used to connect the remote sites of a customer with C-Tag transparency. There are no match criteria for a TLS. **-** If no TLS service is configured on an UNI-P port, all packets not matching any of the service instances configured on the ports will be dropped. If a TLS service is configured, then all packets not matching the other service instances on that port will be tagged as per the TLS definition on that port. TLS service defined by the user will be used by Untagged, Priority Tagged, and C-VLAN tagged packets which do not match any other service instances on the port. **-** If a TLS service is configured on an UNI-S port, service VLAN tagged (including double tagged) frames that do not match other service instances on the port will be forwarded to appropriate NNI port(s) based on the S-VID associated with the service without any VLAN modification. Untagged and priority tagged packets that do not match other service instances on the port will be dropped.
port-list	NNI port list.

2.6 Provisioning (IEEE 802.1p) Commands

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

2.6.1 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

2.6.2 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

2.7 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.

2.7.1 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

2.7.1.1 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

2.7.2 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

2.7.2.1 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

2.7.3 show switchport protected

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

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

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
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.

2.7.4 show interfaces switchport

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

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

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
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>*.

2.8 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).

2.8.1 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>`*

Mode
- Interface Config
- Global Config

2.8.1.1 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`**

Mode
- Interface Config
- Global Config

2.8.2 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>`*

Mode
- Interface Config
- Global Config

2.8.2.1 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`**

Mode
- Interface Config
- Global Config

2.8.3 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>*

Mode
- Interface Config
- Global Config

2.8.3.1 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`

Mode
- Interface Config
- Global Config

2.8.4 show garp

This command displays GARP information.

Format `show garp`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
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.

2.9 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.

2.9.1 set gvrp adminmode

This command enables GVRP on the system.

Default disabled

Format `set gvrp adminmode`
Mode Privileged EXEC

2.9.1.1 no set gvrp adminmode

This command disables GVRP.

Format `no set gvrp adminmode`
Mode Privileged EXEC

2.9.2 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`
Mode
- Interface Config
- Global Config

2.9.2.1 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`
Mode
- Interface Config
- Global Config

2.9.3 show gvrp configuration

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

Format `show gvrp configuration` *{<slot/port> | all}*
Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
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).

Term	*Definition*
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.

2.10 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.

2.10.1 set gmrp adminmode

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

Default disabled

Format `set gmrp adminmode`

Mode Privileged EXEC

2.10.1.1 no set gmrp adminmode

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

Format `no set gmrp adminmode`

Mode Privileged EXEC

2.10.2 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`

Mode
- Interface Config
- Global Config

2.10.2.1 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`

Mode
- Interface Config
- Global Config

2.10.3 show gmrp configuration

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

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

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
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.

2.10.4 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

Term	*Definition*
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.

Term	*Definition*
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:).

2.11 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.

2.11.1 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

2.11.1.1 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

2.11.2 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

2.11.3 clear radius statistics

This command is used to clear all RADIUS statistics.

Format **clear radius statistics**
Mode Privileged EXEC

2.11.4 dot1x default-login

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 default-login** *<listname>*
Mode Global Config

2.11.5 dot1x guest-vlan

This command configures VLAN as guest vlan on a per port basis. The command specifies an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to the maximumVLAN ID supported by the platform.

Default disabled
Format **dot1x guest-vlan** *<vlan-id>*
Mode Interface Config

2.11.5.1 no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default disabled
Format **no dot1x guest-vlan**
Mode Interface Config

2.11.6 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 or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format **dot1x initialize** *<slot/port>*
Mode Privileged EXEC

2.11.7 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

2.11.8 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

2.11.8.1 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

2.11.9 dot1x max-users

Use this command to set the maximum number of clients supported on the port when MAC-based dot1x authentication is enabled on the port. The maximum users supported per port is dependent on the product. The *<count>* value is in the range 1 - 16.

2.11.9.1 no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format **no dot1x max-req**
Mode Interface Config

2.11.10 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. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

Default	auto
Format	**dot1x port-control** *{force-unauthorized | force-authorized | auto | mac-based}*
Mode	Interface Config

2.11.10.1 no dot1x port-control

This command sets the 802.1x port control mode on the specified port to the default value.

Format	**no dot1x port-control**
Mode	Interface Config

2.11.11 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. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	**dot1x port-control all** *{force-unauthorized | force-authorized | auto | mac-based}*
Mode	Global Config

2.11.11.1 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

2.11.12 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 or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

Format	**dot1x re-authenticate** *<slot/port>*
Mode	Privileged EXEC

2.11.13 dot1x re-authentication

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

Default disabled
Format `dot1x re-authentication`
Mode Interface Config

2.11.13.1 no dot1x re-authentication

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

Format `no dot1x re-authentication`
Mode Interface Config

2.11.14 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

2.11.14.1 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

2.11.15 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:

Tokens	*Definition*
guest-vlan-period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
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.

Tokens	*Definition*
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
- guest-vlan-period: 90 seconds
- reauth-period: 3600 seconds
- quiet-period: 60 seconds
- tx-period: 30 seconds
- supp-timeout: 30 seconds
- server-timeout: 30 seconds

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

Mode Interface Config

2.11.15.1 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** *{guest-vlan-period | reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}*

Mode Interface Config

2.11.16 dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with that port. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID. The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

2.11.16.1 no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format **no dot1x unauthenticated-vlan**

Mode Interface Config

2.11.17 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

2.11.17.1 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

2.11.18 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

2.11.19 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

2.11.20 show authentication

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

Format **show authentication**
Mode Privileged EXEC

Term	*Definition*
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.

2.11.21 show authentication methods

Use this command to display information about the authentication methods.

Format **show authentication methods**
Mode Privileged EXEC

Example: The following example displays the authentication configuration.

```
(switch)#show authentication methods

Login Authentication Method Lists
---------------------------------
defaultList         :  local

Enable Authentication Method Lists
----------------------------------
enableList          :  local

Line      Login Method List     Enable Method List
-------   -----------------     ------------------
Console   defaultList           enableList
Telnet    defaultList           enableList
SSH       defaultList           enableList

HTTPS        :local
HTTP         :local
DOT1X        :none
```

2.11.22 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

Term	*Definition*
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.

2.11.23 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 the optional parameters *<unit/slot/port>* or *<vlanid>*, the command displays the global dot1x mode and the VLAN Assignment mode.

Term	*Definition*
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS assigned VLAN is allowed (enabled) or not (disabled).

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

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

Term	*Definition*
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto| mac-based | authorized | unauthorized.
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.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

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

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

Term	*Definition*
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.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto| mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
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.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
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.

Term	*Definition*
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.
Vlan-assigned	The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
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.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

Note: MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

For each client authenticated on the port, the `show dot1x detail <slot/port>` command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

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

Term	*Definition*
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.

Term	Definition
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.

2.11.24 show dot1x clients

This command displays 802.1x client information.

Format **show dot1x clients {***<slot/port>* | all}

Mode Privileged EXEC

Term	Definition
Logical Interface	The logical port number associated with a client.
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

2.11.25 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

Term	*Definition*
Users	Users configured locally to have access to the specified port.

2.12 Storm-Control Commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

FASTPATH provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. 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.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the “no” version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the “no” version of the “storm-control” command (not stating a “level”) disables that form of storm-control but maintains the configured “level” (to be active the next time that form of storm-control is enabled.)

Note: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

2.12.1 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 Global Config
Interface Config

2.12.1.1 no storm-control broadcast

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

Format `no storm-control broadcast`

Mode Global Config
Interface Config

2.12.2 storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for an interface as a percentage of link speed and enable broadcast storm recovery. 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 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

2.12.2.1 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

2.12.3 storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for an interface in packets per second. 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 is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 0

Format `storm-control broadcast rate` *<0-33554431>*

Mode Interface Config

2.12.3.1 no storm-control broadcast rate

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 rate`

Mode Interface Config

2.12.4 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

2.12.4.1 no storm-control broadcast all

This command disables broadcast storm recovery mode for all interfaces.

Format `no storm-control broadcast all`
Mode Global Config

2.12.5 storm-control broadcast all level

This command configures the broadcast storm recovery threshold for all interfaces as a percentage of link speed and enables broadcast storm recovery. 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

2.12.5.1 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

2.12.6 storm-control broadcast all rate

Use this command to configure the broadcast storm recovery threshold for all interfaces in packets per second. 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 is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 0
Format `storm-control broadcast rate` *<0-33554431>*
Mode Global Config

2.12.6.1 no storm-control broadcast all rate

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 rate`
Mode Global Config

2.12.7 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

2.12.7.1 no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Format `no storm-control multicast`
Mode Interface Config

2.12.8 storm-control multicast level

This command configures the multicast storm recovery threshold for an interface as a percentage of link speed 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

2.12.8.1 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` *<0-100>*
Mode Interface Config

2.12.9 storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for an interface in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface

increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default 0
Format **storm-control multicast rate** *<0-33554431>*
Mode Interface Config

2.12.9.1 no storm-control multicast rate

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 rate**
Mode Interface Config

2.12.10 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

2.12.10.1 no storm-control multicast all

This command disables multicast storm recovery mode for all interfaces.

Format **no storm-control multicast all**
Mode Global Config

2.12.11 storm-control multicast all level

This command configures the multicast storm recovery threshold for all interfaces as a percentage of link speed 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

2.12.11.1 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

2.12.12 storm-control multicast all rate

Use this command to configure the multicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default 0
Format **storm-control multicast rate** *<0-33554431>*
Mode Global Config

2.12.12.1 no storm-control broadcast all rate

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 rate**
Mode Global Config

2.12.13 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

2.12.13.1 no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Format **no storm-control unicast**
Mode Interface Config

2.12.14 storm-control unicast level

This command configures the unicast storm recovery threshold for an interface as a percentage of link speed, 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

2.12.14.1 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

2.12.15 storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for an interface in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default 0
Format `storm-control unicast rate` *<0-33554431>*
Mode Interface Config

2.12.15.1 no storm-control unicast rate

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 rate`
Mode Interface Config

2.12.16 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

2.12.16.1 no storm-control unicast all

This command disables unicast storm recovery mode for all interfaces.

Format `no storm-control unicast all`
Mode Global Config

2.12.17 storm-control unicast all level

This command configures the unicast storm recovery threshold for all interfaces as a percentage of link speed 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.

Default 5
Format **`storm-control unicast all level`** *`<0-100>`*
Mode Global Config

2.12.17.1 no storm-control unicast all level

This command sets 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

2.12.18 storm-control unicast all rate

Use this command to configure the unicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default 0
Format **`storm-control unicast all rate`** *`<0-33554431>`*
Mode Global Config

2.12.18.1 no storm-control unicast all rate

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

Format **`no storm-control unicast all rate`**
Mode Global Config

2.12.19 storm-control flowcontrol (AM4910 only)

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

2.12.19.1 no storm-control flowcontrol (AM4910 only)

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

2.12.20 storm-control flowcontrol (AM4904 only)

This command enables 802.3x flow control for the switch and only applies to full-duplex mode ports. The command is extended by parameters to configure flow control (MMU) settings. This is available for AM4910 only. Possible settings are:

- overcommit: overcommit factor for dynamic pool.
- flow-fanin: weight for sending pause/stop frames. Higher values effects sending a pause/stop frame earlier.
- flow-percent:
- Percentage of per-port cells useable before flow control starts.
- static-bytes:
- Per-port/per-cos static reserved limit. Rounded up from bytes to next cell size. Remaining cells are put in dynamic pool. If 0, then “static-percent” is used.
- static-percent:
- Percentage of per-port/per-cos cells to use as static reserved limit. Remaining cells are put in dynamic pool. Only used if “static-bytes” is 0.

To activate new configures values you have to save the configuration and reboot the system.

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
storm-control flowcontrol overcommit <1-5>
storm-control flowcontrol flow-fanin <1-16>
storm-control flowcontrol flow-percent <50-90>
storm-control flowcontrol static-bytes <0,1536-100000>
storm-control flowcontrol static-percent <10-100>
```

Mode Global Config

2.12.20.1 no storm-control flowcontrol (AM4904 only)

This command disables 802.3x flow control for the switch and resets flow control (MMU) settings.

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

Format `no storm-control flowcontrol`
`no storm-control flowcontrol overcommit <1-5>`
`no storm-control flowcontrol flow-fanin <1-16>`
`no storm-control flowcontrol flow-percent <50-90>`
`no storm-control flowcontrol static-bytes <0,1536-100000>`
`no storm-control flowcontrol static-percent <10-100>`

Mode Global Config

2.12.21 show storm-control

This command displays the current used flow control settings and (if existing) the configured flow control settings in parenthesis. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

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

Term	*Definition*
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is 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.

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show storm-control
802.3x Flow Control Mode..................... Disable
```

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show storm-control 1/0/1

        Bcast    Bcast     Mcast    Mcast     Ucast    Ucast
 Intf    Mode     Level     Mode     Level     Mode     Level
------ ------- -------- ------- -------- ------- --------
1/0/1  Disable        5% Disable        5% Disable        5%
```

Example: The following shows an example of part of the CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show storm-control all

        Bcast    Bcast     Mcast    Mcast     Ucast    Ucast
 Intf    Mode     Level     Mode     Level     Mode     Level
------ ------- -------- ------- -------- ------- --------
```

```
1/0/1   Disable       5% Disable       5% Disable       5%
1/0/2   Disable       5% Disable       5% Disable       5%
1/0/3   Disable       5% Disable       5% Disable       5%
1/0/4   Disable       5% Disable       5% Disable       5%
1/0/5   Disable       5% Disable       5% Disable       5%
```

2.12.22 show storm-control flowcontrol

This command displays the current used flow control settings and (if existing) the configured flow control settings in parenthesis. Note that the enable/disable mode is displayed by the standard FASTPATH command “show storm-control”.

Format	**`show storm-control flowcontrol`**
Mode	Privileged EXEC

2.13 Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which is defined in the 802.3AD specification, and that 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.

2.13.1 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 2.1.11 “speed” on page 2 - 6.

Format	**`port-channel`** *<name>*
Mode	Global Config

2.13.1.1 no port-channel

This command deletes a port-channel (LAG).

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

2.13.2 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 2.1.11 “speed” on page 2 - 6.

Format **addport** *<logical slot/port>*
Mode Interface Config

2.13.3 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

2.13.4 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 6.4.7 “clear port-channel” on page 6 - 22.

Format **deleteport** *{<logical slot/port> | all}*
Mode Global Config

2.13.5 lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of <*key*> is 0 to 65535.

Default 0x8000
Format **lacp admin key <***key***>**
Mode Interface Config

Note: This command is only applicable to port-channel interfaces.

2.13.5.1 no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format **no lacp admin key**
Mode Interface Config

2.13.6 lacp collector max-delay

Use this command to configure the port-channel collector max delay. The valid range of <*delay*> is 0-65535.

Default 0x8000

Format **lacp collector max delay <*delay*>**

Mode Interface Config

Note: This command is only applicable to port-channel interfaces.

2.13.6.1 no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format **no lacp collector max delay**

Mode Interface Config

2.13.7 lacp actor admin

Use this command to configure the LACP actor admin parameters.

2.13.8 lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key. The valid range for <*key*> is 0-65535.

Default Internal Interface Number of this Physical Port

Format **lacp actor admin key <*key*>**

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.8.1 no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format **no lacp actor admin key**

Mode Interface Config

2.13.9 lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. The valid value range is 0x00-0xFF.

Default 0x07

Format `lacp actor admin state {individual|longtimeout|passive}`

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.9.1 no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Format `no lacp actor admin state {individual|longtimeout|passive}`

Mode Interface Config

2.13.10 lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format `lacp actor admin state individual`

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.10.1 no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format `no lacp actor admin state individual`

Mode Interface Config

2.13.11 lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format `lacp actor admin state longtimeout`

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.11.1 no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format `no lacp actor admin state longtimeout`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.12 lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format `lacp actor admin state passive`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.12.1 no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format `no lacp actor admin state passive`
Mode Interface Config

2.13.13 lacp actor port

Use this command to configure LACP actor port priority key.

2.13.14 lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port. The valid range for <*priority*> is 0 to 255.

Default 0x80
Format `lacp actor port priority` *<priority>*
Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.14.1 no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format **no lacp actor port priority**
Mode Interface Config

2.13.15 lacp actor system priority

Use this command to configure the priority value associated with the LACP Actor's SystemID. The range for <*priority*> is 0 to 255.

Default 0x80
Format **lacp actor system priority <*priority*>**
Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.15.1 no lacp actor system priority

Use this command to configure the priority value associated with the Actor's SystemID.

Format **lacp actor system priority**
Mode Interface Config

2.13.16 lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. The valid range for <*key*> is 0 to 65535.

Default 0x0
Format **lacp partner admin key <*key*>**
Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.16.1 no lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner.

Format **no lacp partner admin key <*key*>**
Mode Interface Config

2.13.17 lacp partner admin state

Use this command to configure the current administrative value of actor state for the protocol Partner. The valid value range is 0x00-0xFF.

Default 0x07

Format `lacp partner admin state {individual|longtimeout|passive}`

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.17.1 no lacp partner admin state

Use this command the configure the default current administrative value of actor state for the protocol partner.

Format `no lacp partner admin state {individual|longtimeout|passive}`

Mode Interface Config

2.13.18 lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format `lacp partner admin state individual`

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.18.1 no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format `no lacp partner admin state individual`

Mode Interface Config

2.13.19 lacp partner admin state longtimeout

Use this command to set LACP partner admin state to longtimeout.

Format `lacp partner admin state longtimeout`

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.19.1 no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format `no lacp partner admin state longtimeout`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.20 lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format `lacp partner admin state passive`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.20.1 no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format `no lacp partner admin state passive`
Mode Interface Config

2.13.21 lacp partner port id

Use this command to configure the LACP partner port id. The valid range for <*port-id*> is 0 to 65535.

Default 0x80
Format `lacp partner port-id <port-id>`
Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.21.1 no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format `lacp partner port-id`
Mode Interface Config

2.13.22 lacp partner port priority

Use this command to configure the LACP partner port priority. The valid range for <*priority*> is 0 to 255.

Default 0x0

Format **lacp partner port priority <*priority*>**

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.22.1 no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format **no lacp partner port priority**

Mode Interface Config

2.13.23 lacp partner system-id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. The valid range of <*system-id*> is 00:00:00:00:00:00 - FF:FF:FF:FF:FF:FF.

Default 00:00:00:00:00:00

Format **lacp partner system-id <*system-id*>**

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.23.1 no lacp partner system-id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format **no lacp partner system-id**

Mode Interface Config

2.13.24 lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. The valid range for <*priority*> is 0 to 255.

Default 0x0

Format **lacp partner system priority <*priority*>**

Mode Interface Config

Note: This command is only applicable to physical interfaces.

2.13.24.1 no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format `no lacp partner system priority`
Mode Interface Config

2.13.25 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

2.13.25.1 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

2.13.26 port lacpmode

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

Default enabled
Format `port lacpmode`
Mode Interface Config

2.13.26.1 no port lacpmode

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

Format `no port lacpmode`
Mode Interface Config

2.13.27 port lacpmode all

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

Format `port lacpmode all`

Mode Global Config

2.13.27.1 no port lacpmode all

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

Format `no port lacpmode all`
Mode Global Config

2.13.28 port lacptimeout (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 lacptimeout {actor | partner} {long | short}`
Mode Interface Config

2.13.28.1 no port lacptimeout

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 lacptimeout {actor | partner}`
Mode Interface Config

2.13.29 port lacptimeout (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 lacptimeout {actor | partner} {long | short}`
Mode Global Config

2.13.29.1 no port lacptimeout

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 lacptimeout {actor | partner}`
Mode Global Config

2.13.30 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

2.13.30.1 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

2.13.31 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

2.13.31.1 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

2.13.32 port-channel load-balance

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

Default 3

Format **port-channel load-balance** *{ 1 | 2 | 3 | 4 | 5 | 6 } {<slot/port> |<all>}*

Mode Interface Config
Global Config

Term	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
<slot/port>| all	Global Config Mode only: The interface is a logical slot/port number of a configured port-channel. "All" applies the command to all currently configured port-channels.

2.13.32.1 no port-channel load-balance

This command reverts to the default load balancing configuration.

Format **no port-channel load-balance** *{<slot/port> | <all>}*

Mode Interface Config
Global Config

2.13.33 port-channel hash multicast

This command configures the multicast hash algorithm. The command allows the user to globally select the hash algorithm used for distribution of NUC (Non Unicast) traffic. This includes broadcast and multicast traffic, as well as unicast traffic to unknown destination MAC address (DLF, flooded). Traffic distribution may be based on Source address (sa), destination address (da), or port number, or any combination thereof.

Format **port-channel hash multicast** *{sa|sa-port|da|da-port|port|sa-da|sa-da-port}*

Mode Global Config

2.13.34 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

2.13.35 port-channel system priority

Use this command to configure port-channel system priority. The valid range of <priority> is 0-65535.

Default 0x8000

Format **port-channel system priority <***priority***>**

Mode Global Config

2.13.35.1 no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format `no port-channel system priority`

Mode Global Config

2.13.36 show lacp actor

Use this command to display LACP actor attributes.

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

Mode Global Config

The following output parameters are displayed.

Parameter	*Description*
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

2.13.37 show lacp partner

Use this command to display LACP partner attributes.

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

Mode Privileged EXEC

The following output parameters are displayed.

Parameter	*Description*
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	The value representing the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

2.13.38 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`

Mode
- Privileged EXEC
- User EXEC

For each port-channel the following information is displayed:

Term	*Definition*
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.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

2.13.39 show port-channel

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

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

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Logical Interface	Valid slot and port number separated by a forward slash.
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).

2.13.40 show port-channel system priority

Use this command to display the port-channel system priority.

Format `show port-channel system priority`

Mode Privileged EXEC

2.13.41 show port-channel hash multicast

This command displays current port-channel hash multicast settings.

Format `show port-channel hash multicast`

Mode Privileged EXEC

2.14 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.

2.14.1 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

2.14.1.1 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

2.14.2 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

2.14.3 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

Term	*Definition*
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.

2.15 Static MAC Filtering

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

2.15.1 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.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

- For unicast MAC address filters and multicast MAC address filters with source port lists, the maximum number of static MAC filters supported is 20.
- For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 256.

i.e. For current Broadcom platforms, you can configure the following combinations:

- Unicast MAC and source port (max = 20)
- Multicast MAC and source port (max=20)
- Multicast MAC and destination port (only) (max=256)
- Multicast MAC and source ports and destination ports (max=20)

Format **macfilter** *<macaddr> <vlanid>*
Mode Global Config

2.15.1.1 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

2.15.2 macfilter adddest

Use this command to add the interface to the destination filter set for the MAC filter with the given *<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.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format **macfilter adddest <***macaddr***>** *<vlanid>*
Mode Interface Config

2.15.2.1 no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given *<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 adddest <***macaddr***>** *<vlanid>*
Mode Interface Config

2.15.3 macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given *<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.

Note: Configuring a destination port list is only valid for multicast MAC addresses.

Format **macfilter adddest all <***macaddr***>** *<vlanid>*
Mode Global Config

2.15.3.1 no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given *<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 adddest all <***macaddr***>** *<vlanid>*
Mode	Global Config

2.15.4 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

2.15.4.1 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

2.15.5 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

2.15.5.1 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

2.15.6 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

Term	*Definition*
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).

Note: Only multicast address filters will have destination port lists.

2.15.7 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

Term	*Definition*
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. 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:).

2.16 DHCP L2 Relay Agent Commands

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

2.16.1 dhcp l2relay

This command enables the DHCP Layer 2 Relay agent for an interface. The subsequent commands mentioned in this section can only be used when the DHCP L2 relay is enabled.

Format `dhcp l2relay`

Mode
- Global Config
- Interface Config

2.16.1.1 no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface.

Format **no dhcp l2relay**

Mode
- Global Config
- Interface Config

2.16.2 dhcp l2relay circuit-id subscription-name

This command sets the Option-82 Circuit ID for a given service subscription identified by <subscription-string> on a given interface. The <subscription-string> is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is enabled using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 circuit-id as the incoming interface number.

Default disabled

Format **dhcp l2relay circuit-id subscription-name** *<subscription-string>*

Mode Interface Config

2.16.2.1 no dhcp l2relay circuit-id subscription-name

This command resets the Option-82 Circuit ID for a given service subscription identified by <subscription-string> on a given interface. The <subscription-string> is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is disabled using this command, all Client DHCP requests that fall under this service subscription are no longer added with Option-82 circuit-id.

Format **no dhcp l2relay circuit-id subscription-name** *<subscription-string>*

Mode Interface Config

2.16.3 dhcp l2relay circuit-id vlan

This parameter sets the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format **dhcp l2relay circuit-id vlan** *<vlan-list>*

Mode Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

2.16.3.1 no dhcp l2relay circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Format **no dhcp l2relay circuit-id vlan** *<vlan-list>*

Mode Global Config

2.16.4 dhcp l2relay remote-id subscription-name

This command sets the Option-82 Remote-ID string for a given service subscription identified by <subscription-string> on a given interface. The <subscription-string> is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. The <remoteid-string> is a character string. When remote-id string is set using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 Remote-id as the configured remote-id string.

Default empty string

Format **dhcp l2relay remote-id** *<remoteid-string>* **subscription-name** *<subscription-string>*

Mode Interface Config

2.16.4.1 no dhcp l2relay remote-id subscription-name

This command resets the Option-82 Remote-ID string for a given service subscription identified by <subscription-string> on a given interface. The <subscription-string> is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When remote-id string is reset using this command, the Client DHCP requests that fall under this service subscription are not added with Option-82 Remote-id.

Format **no dhcp l2relay remote-id** *<remoteid-string>* **subscription-name** *<subscription-string>*

Mode Interface Config

2.16.5 dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format **dhcp l2relay remote-id** *<remote-id-string>* **vlan** *<vlan-list>*

Mode Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

2.16.5.1 no dhcp l2relay remote-id vlan

This parameter clears the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format **no dhcp l2relay remote-id vlan** *<vlan-list>*

Mode Global Config

2.16.6 dhcp l2relay subscription-name

This command enables relaying DHCP packets that fall under the specified service subscription. The <subscription-string> is a character string that needs to be matched with configured DOT1AD subscription string for correct operation.

Default	disabled (i.e. no DHCP packets are relayed)
Format	**dhcp l2relay subscription-name** *<subscription-string>*
Mode	Interface Config

2.16.6.1 no dhcp l2relay subscription-name

This command disables relaying DHCP packets that fall under the specified service subscription. The <subscription-string> is a character string that needs to be matched with configured DOT1AD subscription string for correct operation.

Format	**no dhcp l2relay subscription-name** *<subscription-string>*
Mode	Interface Config

2.16.7 dhcp l2relay trust

Use this command to configure an interface as trusted for Option-82 reception.

Default	untrusted
Format	**dhcp l2relay trust**
Mode	Interface Config

2.16.7.1 no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format	**no dhcp l2relay trust**
Mode	Interface Config

2.16.8 dhcp l2relay vlan

Use this command to enable the DHCP L2 Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default	disable
Format	**dhcp l2relay vlan** <vlan-list>
Mode	Global Config

Parameter	*Description*
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

2.16.8.1 no dhcp l2relay vlan

Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Format	**no dhcp l2relay vlan** *<vlan-list>*
Mode	Global Config

2.16.9 show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Format **show dhcp l2relay all**

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show dhcp l2relay all

DHCP L2 Relay is  Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted

VLAN Id    L2 Relay  CircuitId  RemoteId
--------- ----------  ----------- ------------
 3          Disabled    Enabled    --NULL--
 5          Enabled     Enabled    --NULL--
 6          Enabled     Enabled    broadcom
 7          Enabled     Disabled   --NULL--
 8          Enabled     Disabled   --NULL--
 9          Enabled     Disabled   --NULL--
 10         Enabled     Disabled   --NULL--
```

2.16.10 show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Format **show dhcp l2relay interface** *{all|<interface-num>}*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show dhcp l2relay interface all

DHCP L2 Relay is  Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted
```

2.16.11 show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Format **show dhcp l2relay stats interface** *{all|<interface-num>}*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show dhcp l2relay stats interface all

DHCP L2 Relay is  Enabled.

Interface  UntrustedServer    UntrustedClient  TrustedServer     TrustedClient
            MsgsWithOpt82    MsgsWithOpt82    MsgsWithoutOpt82  MsgsWithoutOpt82
---------  ---------------- -----------------  ----------------- --------------
 0/1           0                 0                 0                0
 0/2           0                 0                 3                7
 0/3           0                 0                 0                0
 0/4           0                 12                0                0
 0/5           0                 0                 0                0
 0/6           3                 0                 0               0
 0/7           0                 0                 0                0
 0/8           0                 0                 0                0
 0/9           0                 0                 0                0
```

2.16.12 show dhcp l2relay subscription interface

This command displays DHCP L2 Relay configuration specific to a service subscription on an interface.

Format **show dhcp l2relay subscription interface** *{all|<interface-num>}*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

(FASTPATH Switching) #show dhcp l2relay subscription interface all

```
Interface   SubscriptionName    L2Relay mode  Circuit-Id mode  Remote-Id mode
----------  ----------------   -------------- ---------------  ----------------
  0/1             sub1             Enabled       Disabled         --NULL--
  0/2             sub3             Enabled       Disabled         EnterpriseSwitch
  0/2             sub22            Disabled      Enabled          --NULL--
  0/4             sub4             Enabled       Enabled          --NULL--
```

2.16.13 show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format **show dhcp l2relay agent-option vlan** *<vlan-range>*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show dhcp l2relay agent-option vlan 5-10

DHCP L2 Relay is  Enabled.

VLAN Id    L2 Relay    CircuitId  RemoteId
--------- ----------  ----------- ------------
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    broadcom
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

2.17 DHCP Client Commands

FASTPATH can include vendor and configuration information in DHCP client requests relayed to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

2.17.1 dhcp client vendor-id-option

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the FASTPATH switch.

Format `dhcp client vendor-id-option <string>`
Mode Global Config

2.17.1.1 no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the FASTPATH switch.

Format `no dhcp client vendor-id-option`
Mode Global Config

2.17.2 dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the FASTPATH switch.

Format `dhcp client vendor-id-option-string <string>`
Mode Global Config

2.17.2.1 no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format **`no dhcp client vendor-id-option-string`**
Mode Global Config

2.17.3 show dhcp client vendor-id-option

This command displays the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in DHCP requests.

Format **`show dhcp client vendor-id-option`**
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Switching) #show dhcp client vendor-id-option

DHCP Client Vendor Identifier Option is Enabled
DHCP Client Vendor Identifier Option string is FastpathClient.
```

2.17.4 ip dhcp force-client-id

This feature allows the manipulation of DHCP packets related to the receiving port and (optional and only if Layer3-functionality provided) VLAN.

This command enables the manipulation of a DHCP packet. If enabled a new client identifier is added either the specified one or (if not specified) a default identifier, containing the related slot/port. The manipulation can be done independent of the VLAN or for a special VLAN (only if Layer-3 functionality is provided). First VLAN related specifications are used before the general rule is used. Maximal 32 rules can be specified for a port.

Format
```
ip dhcp force-client-id
ip dhcp force-client-id <identifier>
ip dhcp force-client-id vlan <1-4093>
ip dhcp force-client-id vlan <1-4093> <identifier>
```

Mode Interface Config

2.17.4.1 no ip dhcp force-client-id

This command disables the manipulation of a DHCP packet.

Format
```
no ip dhcp force-client-id
no ip dhcp force-client-id vlan <1-4093>
```

Mode Interface Config

2.17.5 show ip dhcp force-client-id

This command displays the mode (enabled/disabled) and the related VLAN and client-identifier for a specified interface (<slot/port>) or for all physical interfaces.

Format
```
show ip dhcp force-client-id { all | <slot/port>}
```

Mode Privileged Exec

2.17.6 clear ip dhcp force-client-id

This command clears all configured manipulation rules for DHSP packets for all interfaces.

Format
```
clear ip dhcp force-client-id
```

Mode Privileged Exec

2.18 Dynamic ARP Inspection Commands

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station’s IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

2.18.1 ip arp inspection vlan

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default `disabled`
Format **`ip arp inspection vlan vlan-list`**
Mode Global Config

2.18.1.1 no ip arp inspection vlan

Use this command to disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Format **`no ip arp inspection vlan vlan-list`**
Mode Global Config

2.18.2 ip arp inspection validate

Use this command to enable additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables src-mac and dst-mac validations, and a second command enables IP validation only, the src-mac and dst-mac validations are disabled as a result of the second command.

Default `disabled`
Format **`ip arp inspection validate {[src-mac] [dst-mac] [ip]}`**
Mode Global Config

2.18.2.1 no ip arp inspection validate

Use this command to disable the additional validation checks on the received ARP packets.

Format **`no ip arp inspection validate {[src-mac] [dst-mac] [ip]}`**
Mode Global Config

2.18.3 ip arp inspection vlan logging

Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default `enabled`
Format **`ip arp inspection vlan vlan-list logging`**
Mode Global Config

2.18.3.1 no ip arp inspection vlan logging

Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format `no ip arp inspection vlan vlan-list logging`
Mode Global Config

2.18.4 ip arp inspection trust

Use this command to configure an interface as trusted for Dynamic ARP Inspection.

Default `enabled`
Format `ip arp inspection trust`
Mode Interface Config

2.18.4.1 no ip arp inspection trust

Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format `no ip arp inspection trust`
Mode Interface Config

2.18.5 ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections. The maximum pps value shown in the range for the rate option might be more than the hardware allowable limit. Therefore you need to understand the switch performance and configure the maximum rate pps accordingly.

Note: The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.

Default `15 pps for rate and 1 second for burst-interval`
Format `ip arp inspection limit {rate pps [burst interval seconds] | none}`
Mode Interface Config

2.18.5.1 no ip arp inspection limit

Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format `no ip arp inspection limit`
Mode Interface Config

2.18.6 ip arp inspection filter

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Default `No ARP ACL is configured on a VLAN`

Format `ip arp inspection filter acl-name vlan vlan-list [static]`
Mode Global Config

2.18.6.1 no ip arp inspection filter

Use this command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format `no ip arp inspection filter acl-name vlan vlan-list [static]`
Mode Global Config

2.18.7 arp access-list

Use this command to create an ARP ACL.

Format `arp access-list acl-name`
Mode Global Config

2.18.7.1 no arp access-list

Use this command to delete a configured ARP ACL.

Format `no arp access-list acl-name`
Mode Global Config

2.18.8 permit ip host mac host

Use this command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format `permit ip host sender-ip mac host sender-mac`
Mode ARP Access-list Config

2.18.8.1 no permit ip host mac host

Use this command to delete a rule for a valid IP and MAC combination.

Format `no permit ip host sender-ip mac host sender-mac`
Mode ARP Access-list Config

2.18.9 show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the *vlan-list* argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the **source mac validation**, **destination mac validation** and **invalid IP validation** information.

Format `show ip arp inspection [vlan <vlan-list>]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

Example: The following shows example CLI display output for the command.

```
(Switching) #show ip arp inspection vlan 10-12

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan          Configuration    Log Invalid   ACL Name   Static flag
 ----          -------------    -----------   ---------  -----------
   10               Enabled        Enabled   H2         Enabled
   11              Disabled        Enabled
   12              Enabled        Disabled
```

2.18.10 show ip arp inspection statistics

Use this command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format `show ip arp inspection statistics [vlan vlan-list]`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
VLAN	The VLAN ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.

Term	*Definition*
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

Example: The following shows example CLI display output for the command **show ip arp inspection statistics** which lists the summary of forwarded and dropped ARP packets on all DAI-enabled VLANs.

```
VLAN  Forwarded  Dropped
----  ---------  -------
  10         90       14
  20         10        3
```

Example: The following shows example CLI display output for the command **show ip arp inspection statistics vlan <*vlan-list*>**.

```
VLAN    DHCP       ACL        DHCP       ACL       Bad Src    Bad Dest    Invalid
        Drops      Drops      Permits    Permits     MAC        MAC         IP
----- -------- --------- ----------- --------- ---------- ----------- ---------
10      11         1           65         25          1          1          0
20      1          0            8          2          0          1          1
```

2.18.11 clear ip arp inspection statistics

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Default none

Format **clear ip arp inspection statistics**

Mode Privileged EXEC

2.18.12 show ip arp inspection interfaces

Use this command to display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a slot/port interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format **show ip arp inspection interfaces [slot/port]**

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

Example: The following shows example CLI display output for the command.

```
(Switching) #show ip arp inspection interfaces

 Interface       Trust State   Rate Limit   Burst Interval
                                    (pps)         (seconds)
 --------------  -----------   ----------   ---------------
 0/1                Untrusted           15                1
 0/2                Untrusted           10               10
```

2.18.13 show arp access-list

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format	**`show arp access-list [acl-name]`**
Mode	• Privileged EXEC • User EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show arp access-list

ARP access list H2
    permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
    permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
ARP access list H3
ARP access list H4
    permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```

2.19 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.

2.19.1 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`**

Mode
- Global Config
- Interface Config

Format **`set igmp`** *<vlanid>*

Mode VLAN Config

2.19.1.1 no set igmp

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

Format **`no set igmp`**

Mode
- Global Config
- Interface Config

Format **`no set igmp`** *<vlanid>*

Mode VLAN Config

2.19.2 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

2.19.2.1 no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format **`no set igmp interfacemode`**

Mode Global Config

2.19.3 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

2.19.3.1 no set igmp fast-leave

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

Format **`no set igmp fast-leave`**

Mode Interface Config

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

Mode VLAN Config

2.19.4 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>*

Mode
- Interface Config
- Global Config

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

Mode VLAN Config

2.19.4.1 no set igmp groupmembership-interval

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

Format **`no set igmp groupmembership-interval`**

Mode
- Interface Config
- Global Config

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

Mode VLAN Config

2.19.5 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 25 seconds.

Default 10 seconds

Format **`set igmp maxresponse`** *`<1-25>`*

Mode
- Global Config
- Interface Config

Format **`set igmp maxresponse`** *`<vlan_id> <1-25>`*

Mode VLAN Config

2.19.5.1 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`**

Mode
- Global Config
- Interface Config

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

Mode VLAN Config

2.19.6 set igmp mcrtrexpiretime

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 mcrtrexpiretime`** *`<0-3600>`*

Mode
- Global Config
- Interface Config

Format **`set igmp mcrtrexpiretime`** *`<vlan_id> <0-3600>`*

Mode VLAN Config

2.19.6.1 no set igmp mcrtrexpiretime

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 mcrtrexpiretime`**

Mode
- Global Config
- Interface Config

Format **no set igmp mcrtrexpiretime** *<vlan_id>*
Mode VLAN Config

2.19.7 set igmp mrouter

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

Format **set igmp mrouter <***vlan_id***>**
Mode Interface Config

2.19.7.1 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

2.19.8 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

2.19.8.1 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

2.19.9 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:

Term	*Definition*
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.

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

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

Term	Definition
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:

Term	Definition
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates 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.

2.19.10 show igmpsnooping mrouter interface

This command displays information about statically configured ports.

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

Mode Privileged EXEC

Term	Definition
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.

2.19.11 show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format **show igmpsnooping mrouter vlan** *<slot/port>*
Mode Privileged EXEC

Term	*Definition*
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

2.19.12 show igmpsnooping proxy-report

This command displays the IGMP proxy-report configuration. The setting can be displayed for a specific (slot/port) or all physical and port-channel interfaces. The displayed fields are

- the setting of proxy-report feature (enable/disable)
- the VLAN awareness for forwarding IGMP messages (only if proxy-report feature is enabled)
- For information: If unregistered multicast messages are flooded at this port or not (see feature
- KEX_CONFIGURE_PORT_MULTICAST_FLOOD, only if feature is enabled).

Format **show igmpsnooping proxy-report** *{all | <slot|port>}*
Mode Privileged EXEC

2.19.13 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

Term	*Definition*
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:).

2.20 IGMP Snooping Querier Commands

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

2.20.1 set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

Note: The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default disabled

Format `set igmp querier [<vlan-id>] [address ipv4_address]`

Mode
- Global Config
- VLAN Mode

2.20.1.1 no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional *address* parameter to reset the querier address to 0.0.0.0.

Format `no set igmp querier [<vlan-id>] [address]`

Mode
- Global Config
- VLAN Mode

2.20.2 set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default disabled

Format **`set igmp querier query-interval`** *<1-18000>*

Mode Global Config

2.20.2.1 no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format **`no set igmp querier query-interval`**

Mode Global Config

2.20.3 set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default 60 seconds

Format **set igmp querier timer expiry** *<60-300>*

Mode Global Config

2.20.3.1 no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format **no set igmp querier timer expiry**

Mode Global Config

2.20.4 set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default 1

Format **set igmp querier version** *<1-2>*

Mode Global Config

2.20.4.1 no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format **no set igmp querier version**

Mode Global Config

2.20.5 set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default disabled

Format **set igmp querier election participate**

Mode VLAN Config

2.20.5.1 no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format **no set igmp querier election participate**

Mode VLAN Config

2.20.6 show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format `show igmpsnooping querier [{detail | vlan <vlanid>}]`

Mode Privileged EXEC

When the optional argument <*vlanid*> is not used, the command displays the following information.

Field	*Description*
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for <*vlanid*>, the following additional information appears.

Field	*Description*
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in “Querier” or “Non-Querier” state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument *detail* is used, the command shows the global information and the information for all Querier-enabled VLANs.

2.21 MLD Snooping Commands

This section describes commands used for MLD Snooping. In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast addresses. In IPv6, MLD Snooping performs a similar function. With MLD Snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

2.21.1 set mld

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

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

MLD Snooping supports the following activities:

- Validation of address version, payload length consistencies and discarding of the frame upon error.
- Maintenance of the forwarding table entries based on the MAC address versus the IPv6 address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default disabled

Format **`set mld`** *`<vlanid>`*

Mode
- Global Config
- Interface Config
- VLAN Mode

2.21.1.1 no set mld

Use this command to disable MLD Snooping on the system.

Format **`set mld`** *`<vlanid>`*

Mode
- Global Config
- Interface Config
- VLAN Mode

2.21.2 set mld interfacemode

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

Default disabled

Format **`set mld interfacemode`**

Mode Global Config

2.21.2.1 no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Format **`no set mld interfacemode`**

Mode Global Config

2.21.3 set mld fast-leave

Use this command to enable MLD 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 and MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

Note: 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.

Note: Fast-leave processing is supported only with MLD version 1 hosts.

Default disabled

Format **`set mld fast-leave`** *<vlanid>*

Mode
- Interface Config
- VLAN Mode

2.21.3.1 no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface.

Format **`no set mld fast-leave`** *<vlanid>*

Mode
- Interface Config
- VLAN Mode

2.21.4 set mld groupmembership-interval

Use this command to set the MLD 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 MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

Default 260 seconds

Format **`set mld groupmembership-interval`** *<vlanid> <2-3600>*

Mode
- Interface Config
- Global Config
- VLAN Mode

2.21.4.1 no set groupmembership-interval

Use this command to set the MLDv2 Group Membership Interval time to the default value.

Format **`no set mld groupmembership-interval`**

Mode
- Interface Config
- Global Config
- VLAN Mode

2.21.5 set mld maxresponse

Use this command to set the MLD Maximum Response time for the system, 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 MLD Query Interval time value. The range is 1 to 65 seconds.

Default 10 seconds

Format **`set mld maxresponse`** *`<1-65>`*

Mode
- Global Config
- Interface Config
- VLAN Mode

2.21.5.1 no set mld maxresponse

Use this command to set the max response time (on the interface or VLAN) to the default value.

Format **`no set mld maxresponse`**

Mode
- Global Config
- Interface Config
- VLAN Mode

2.21.6 set mld mcrtexpiretime

Use this command to set 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 timeout, i.e. no expiration.

Default 0

Format **`set mld mcrtexpiretime`** *`<vlanid> <0-3600>`*

Mode
- Global Config
- Interface Config

2.21.6.1 no set mld mcrtexpiretime

Use this command to set 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 mld mcrtexpiretime`** *`<vlanid>`*

Mode
- Global Config
- Interface Config

2.21.7 set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format **`set mld mrouter`** *`<vlanid>`*

Mode Interface Config

2.21.7.1 no set mld mrouter

Use this command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

Format **no set mld mrouter** *<vlanid>*
Mode Interface Config

2.21.8 set mld mrouter interface

Use this command to configure the interface as a multicast router-attached interface. When configured as a multicast router interface, the interface is treated as a multicast router-attached interface in all VLANs.

Default disabled
Format **set mld mrouter interface**
Mode Interface Config

2.21.8.1 no set mld mrouter interface

Use this command to disable the status of the interface as a statically configured multicast router-attached interface.

Format **no set mld mrouter interface**
Mode Interface Config

2.21.9 show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Format **show mldsnooping** *[<unit/slot/port> | <vlanid>]*
Mode Privileged EXEC

When the optional arguments *<unit/slot/port>* or *<vlanid>* are not used, the command displays the following information.

Term	*Definition*
Admin Mode	Indicates whether or not MLD Snooping is active on the switch.
Interfaces Enabled for MLD Snooping	Interfaces on which MLD Snooping is enabled.
MLD Control Frame Count	Displays the number of MLD Control frames that are processed by the CPU.
VLANs Enabled for MLD Snooping	VLANs on which MLD Snooping is enabled.

When you specify the *<unit/slot/port>* values, the following information displays.

Term	*Definition*
MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the interface.
Fast Leave Mode	Indicates whether MLD Snooping Fast Leave is active on the VLAN.

Term	Definition
Group Membership Interval	Shows 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.
Max Response Time	Displays 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 Present Expiration Time	Displays 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.

When you specify a value for *<vlanid>*, the following information appears.

Term	Definition
VLAN Admin Mode	Indicates whether MLD Snooping is active on the VLAN.

2.21.10 show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

Format **show mldsnooping mrouter interface** *<unit/slot/port>*

Mode Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	Displays the list of VLANs of which the interface is a member.

2.21.11 show mldsnooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

Format **show mldsnooping mrouter vlan** *<unit/slot/port>*

Mode Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

2.21.12 show mac-address-table mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format **show mac-address-table mldsnooping**

Mode Privileged EXEC

Term	*Definition*
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 33:33:45:67:89:AB. In an IVL system, the MAC address is displayed as a MAC address and a VLAN ID combination of 8 bytes.
Type	The type of 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:).

2.22 MLD Snooping Querier Commands

In an IPv6 environment, MLD Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the MLD Querier. The MLD query responses, known as MLD reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes the commands you use to configure and display information on MLD Snooping queries on the network and, separately, on VLANs.

2.22.1 set mld querier

Use this command to enable MLD Snooping Querier on the system (Global Config Mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as a source address while generating periodic queries.

If a VLAN has MLD Snooping Querier enabled and MLD Snooping is operationally disabled on it, MLD Snooping Querier functionality is disabled on that VLAN. MLD Snooping functionality is re-enabled if MLD Snooping is operational on the VLAN.

The MLD Snooping Querier sends periodic general queries on the VLAN to solicit membership reports.

Default disabled

Format **set mld querier** [<*vlan-id*>] [**address** *ipv6_address*]

Mode
- Global Config
- VLAN Mode

2.22.1.1 no set mld querier

Use this command to disable MLD Snooping Querier on the system. Use the optional parameter *address* to reset the querier address.

Format **no set mld querier** [<*vlan-id*>][**address**]

Mode
- Global Config
- VLAN Mode

2.22.2 set mld querier query_interval

Use this command to set the MLD Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default disabled
Format **set mld querier query_interval** *<1-18000>*
Mode Global Config

2.22.2.1 no set mld querier query_interval

Use this command to set the MLD Querier Query Interval time to its default value.

Format **no set mld querier query_interval**
Mode Global Config

2.22.3 set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default 60 seconds
Format **set mld querier timer expiry** *<60-300>*
Mode Global Config

2.22.3.1 no set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period to its default value.

Format **no set mld querier timer expiry**
Mode Global Config

2.22.4 set mld querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default disabled
Format **set mld querier election participate**
Mode VLAN Config

2.22.4.1 no set mld querier election participate

Use this command to set the snooping querier not to participate in querier election but go into a non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format **no set mld querier election participate**
Mode VLAN Config

2.22.5 show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Format **show mldsnooping querier [{detail | vlan <*vlanid*>}]**

Mode Privileged EXEC

When the optional arguments <*vlandid*> are not used, the command displays the following information.

Field	*Description*
Admin Mode	Indicates whether or not MLD Snooping Querier is active on the switch.
Admin Version	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to `MLD v1` and it cannot be changed.
Querier Address	Shows the IP address which will be used in the IPv6 header while sending out MLD queries. It can be configured using the appropriate command.
Query Interval	Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for <*vlanid*>, the following information appears.

Field	*Description*
VLAN Admin Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether MLD Snooping Querier is in "*Querier*" or "*Non-Querier*" state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to *Querier* state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participate	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv6 header while sending out MLD queries on this VLAN. It can be configured using the appropriate command.
Operational Version	This version of IPv6 will be used while sending out MLD queriers on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the MLD version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument *detail* is used, the command shows the global information and the information for all Querier-enabled VLANs.

2.23 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 7.9.7 “snmp-server enable traps violation” on page 7 - 30.

2.23.1 port-security

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

Default disabled

Format `port-security`

Mode
- Global Config
- Interface Config

2.23.1.1 no port-security

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

Format `no port-security`

Mode
- Global Config
- Interface Config

2.23.2 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

2.23.2.1 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

2.23.3 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

2.23.3.1 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

2.23.4 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

2.23.4.1 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

2.23.5 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

2.23.6 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

Term	*Definition*
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:

Term	*Definition*
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.

2.23.7 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

Term	*Definition*
MAC Address	MAC Address of dynamically locked MAC.

2.23.8 show port-security static

This command displays the statically locked MAC addresses for port.

Format **show port-security static** *<slot/port>*
Mode Privileged EXEC

Term	*Definition*
MAC Address	MAC Address of statically locked MAC.

2.23.9 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

Term	*Definition*
MAC Address	MAC Address of discarded packet on locked port.

2.24 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.

2.24.1 lldp transmit

Use this command to enable the LLDP advertise capability.

Default disabled
Format **lldp transmit**
Mode Interface Config

2.24.1.1 no lldp transmit

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

Format **no lldp transmit**
Mode Interface Config

2.24.2 lldp receive

Use this command to enable the LLDP receive capability.

Default disabled
Format **lldp receive**
Mode Interface Config

2.24.2.1 no lldp receive

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

Format **no lldp receive**
Mode Interface Config

2.24.3 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

2.24.3.1 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

2.24.4 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 7.9.1 “snmp-server“on page 7 - 28. 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 2.1.7 “description“on page 2 - 4.

Default no optional TLVs are included

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

Mode Interface Config

2.24.4.1 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

2.24.5 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

2.24.5.1 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

2.24.6 lldp notification

Use this command to enable remote data change notifications.

Default disabled

Format **lldp notification**

Mode Interface Config

2.24.6.1 no lldp notification

Use this command to disable notifications.

Default disabled

Format **no lldp notification**

Mode Interface Config

2.24.7 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

2.24.7.1 no lldp notification-interval

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

Format **no lldp notification-interval**

Mode Global Config

2.24.8 clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format **clear lldp statistics**

Mode Privileged Exec

2.24.9 clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format **clear lldp remote-data**

Mode Global Config

2.24.10 show lldp

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

Format **show lldp**

Mode Privileged Exec

Term	*Definition*
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.

2.24.11 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

Term	*Definition*
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.

2.24.12 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

Term	*Definition*
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:

Term	*Definition*
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.

2.24.13 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

Term	*Definition*
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.

Example: The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show lldp remote-device all

LLDP Remote Device Summary

Local
Interface RemID    Chassis ID            Port ID             System Name
-------  -------   --------------------  ------------------  ------------------
0/1
0/2
0/3
0/4
0/5
0/6
0/7         2      00:FC:E3:90:01:0F     00:FC:E3:90:01:11
0/7         3      00:FC:E3:90:01:0F     00:FC:E3:90:01:12
0/7         4      00:FC:E3:90:01:0F     00:FC:E3:90:01:13
0/7         5      00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7         1      00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7         6      00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

2.24.14 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

Term	*Definition*
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.

Term	*Definition*
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.

Example: The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show lldp remote-device detail 0/7

LLDP Remote Device Detail

Local Interface: 0/7


Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds
```

2.24.15 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

Term	*Definition*
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.

2.24.16 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

Term	*Definition*
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.

2.25 LLDP-MED Commands

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

2.25.1 lldp med

Use this command to enable MED. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default disabled

Format **lldp med**

Mode Interface Config

2.25.1.1 no lldp med

Use this command to disable MED.

Format **no lldp med**

Mode Interface Config

2.25.2 lldp med confignotification

Use this command to configure all the ports to send the topology change notification.

Default disabled

Format **`lldp med confignotification`**

Mode Interface Config

2.25.2.1 no ldp med confignotification

Use this command to disable notifications.

Format **`no lldp med confignotification`**

Mode Interface Config

2.25.3 lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format **`lldp med transmit-tlv`** *`[capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`*

Mode Interface Config

Term	*Definition*
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

2.25.3.1 no lldp med transmit-tlv

Use this command to remove a TLV.

Format **`no lldp med transmit-tlv`** *`[capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`*

Mode Interface Config

2.25.4 lldp med all

Use this command to configure LLDP-MED on all the ports.

Format **`lldp med all`**

Mode Global Config

2.25.5 lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format **lldp med confignotification all**

Mode Global Config

2.25.6 lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. *[count]* is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default 3

Format **lldp med faststartrepeatcount** *[count]*

Mode Global Config

2.25.6.1 no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format **no lldp med faststartrepeatcount**

Mode Global Config

2.25.7 lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format **lldp med transmit-tlv all** *[capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]*

Mode Global Config

Term	*Definition*
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

2.25.7.1 no lldp med transmit-tlv

Use this command to remove a TLV.

Format **no lldp med transmit-tlv** *[capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]*

Mode Global Config

2.25.8 show lldp med

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

Format **show lldp med**

Mode Privileged Exec

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count:  3
Device Class:  Network Connectivity

(Broadcom FASTPATH Routing) #
```

2.25.9 show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. *<slot/port>* indicates a specific physical interface. *all* indicates all valid LLDP interfaces.

Format **show lldp med interface** *{slot/port | all}*

Mode Privileged Exec

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
0/1        Down    Disabled  Disabled  Disabled     0,1
0/2        Up      Disabled  Disabled  Disabled     0,1
0/3        Down    Disabled  Disabled  Disabled     0,1
0/4        Down    Disabled  Disabled  Disabled     0,1
0/5        Down    Disabled  Disabled  Disabled     0,1
0/6        Down    Disabled  Disabled  Disabled     0,1
0/7        Down    Disabled  Disabled  Disabled     0,1
0/8        Down    Disabled  Disabled  Disabled     0,1
0/9        Down    Disabled  Disabled  Disabled     0,1
0/10       Down    Disabled  Disabled  Disabled     0,1
0/11       Down    Disabled  Disabled  Disabled     0,1
0/12       Down    Disabled  Disabled  Disabled     0,1
0/13       Down    Disabled  Disabled  Disabled     0,1
0/14       Down    Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(Broadcom FASTPATH Routing) #show lldp med interface 1/0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
0/2        Up      Disabled  Disabled  Disabled     0,1
```

```
TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory

(Broadcom FASTPATH Routing) #
```

2.25.10 show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. *<slot/port> indicates a specific physical interface.*

Format **show lldp med local-device detail** *<slot/port>*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show lldp med local-device detail 1/0/8

LLDP MED Local Device Detail

Interface: 1/0/8

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
```

```
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

2.25.11 show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format **show lldp med remote-device** *{<slot/port> | all}*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Remote ID  Device Class
---------  ---------  ------------
0/8        1          Class I
0/9        2          Not Defined
0/10       3          Class II
0/11       4          Class III
0/12       5          Network Con
```

2.25.12 show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format **show lldp med remote-device detail** *<slot/port>*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show lldp med remote-device detail 1/0/8

LLDP MED Remote Device Detail

Local Interface: 1/0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type : voice
```

```
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

2.26 Denial of Service Commands

Note: Denial of Service (DataPlane) is supported on XGS-III and later platforms only.

This section describes the commands you use to configure Denial of Service (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 these 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.

Note: Monitoring and blocking of the types of attacks listed below are only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

- **SMAC = DMAC:** Source MAC address = Destination MAC address.
- TCP Port: Source TCP Port = Destination TCP Port.
- UDP Port: Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence:** 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.
- **TCP Offset:** TCP Header Offset = 1.
- **TCP SYN:** TCP Flag SYN set.
- **TCP SYN & FIN:** TCP Flags SYN and FIN set.
- **TCP FIN & URG & PSH:** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6**: Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment**: Checks for fragmented ICMP packets.

2.26.1 dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Format	`dos-control all`
Mode	Global Config

2.26.1.1 no dos-control all

This command disables Denial of Service prevention checks globally.

Format	`no dos-control all`
Mode	Global Config

2.26.2 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

2.26.2.1 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

2.26.3 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

2.26.3.1 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

2.26.4 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

2.26.4.1 no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

Format `no dos-control tcpfrag`
Mode Global Config

2.26.5 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

2.26.5.1 no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format **`no dos-control tcpflag`**

Mode Global Config

2.26.6 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

2.26.6.1 no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format **`no dos-control l4port`**

Mode Global Config

2.26.7 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

2.26.7.1 no dos-control icmp

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format `no dos-control icmp`
Mode Global Config

2.26.8 dos-control smacdmac

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default disabled
Format `dos-control smacdmac`
Mode Global Config

2.26.8.1 no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection.

Format `no dos-control smacdmac`
Mode Global Config

2.26.9 dos-control tcpport

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Default disabled
Format `dos-control tcpport`
Mode Global Config

2.26.9.1 no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format `no dos-control smacdmac`
Mode Global Config

2.26.10 dos-control udpport

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control udpport`
Mode	Global Config

2.26.10.1 no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format	`no dos-control udpport`
Mode	Global Config

2.26.11 dos-control tcpflagseq

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. 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 tcpflagseq`
Mode	Global Config

2.26.11.1 no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	`no dos-control tcpflagseq`
Mode	Global Config

2.26.12 dos-control tcpoffset

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default disabled
Format `dos-control tcpoffset`
Mode Global Config

2.26.12.1 no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format `no dos-control tcpoffset`
Mode Global Config

2.26.13 dos-control tcpsyn

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default disabled
Format `dos-control tcpsyn`
Mode Global Config

2.26.13.1 no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format `no dos-control tcpsyn`
Mode Global Config

2.26.14 dos-control tcpsynfin

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default disabled
Format `dos-control tcpsynfin`
Mode Global Config

2.26.14.1 no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format `no dos-control tcpsynfin`
Mode Global Config

2.26.15 dos-control tcpfinurgpsh

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default disabled
Format `dos-control tcpfinurgpsh`
Mode Global Config

2.26.15.1 no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format `no dos-control tcpfinurgpsh`
Mode Global Config

2.26.16 dos-control icmpv4

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 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 icmpv4` *<0-16384>*
Mode Global Config

2.26.16.1 no dos-control icmpv4

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format `no dos-control icmpv4`
Mode Global Config

2.26.17 dos-control icmpv6

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 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 icmpv6`** *`<0-16384>`*

Mode Global Config

2.26.17.1 no dos-control icmpv6

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format **`no dos-control icmpv6`**

Mode Global Config

2.26.18 dos-control icmpfrag

Note: This command is only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

This command enables ICMP 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 fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default disabled

Format **`dos-control icmpfrag`**

Mode Global Config

2.26.18.1 no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format **`no dos-control icmpfrag`**

Mode Global Config

2.26.19 show dos-control

This command displays Denial of Service configuration information.

Format **`show dos-control`**

Mode Privileged EXEC

Note: Some of the information below displays only if you are using the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.

Term	*Definition*
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0-255>	The factory default is 20.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Pkt Size	The range is 0-1023. The factory default is 512.
Max ICMPv6 Pkt Size	The range is 0-16384. The factory default is 512.
ICMP Fragment Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
TCP Port Mode	May be enabled or disabled. The factory default is disabled.
UDP Port Mode	May be enabled or disabled. The factory default is disabled.
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
SMACDMAC Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
TCP FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

2.27 MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

2.27.1 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

2.27.1.1 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

2.27.2 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

Term	*Definition*
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. •

2.27.3 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

Term	*Definition*
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.

2.27.4 show mac-address-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format `show mac-address-table stats`

Mode Privileged EXEC

Term	*Definition*
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.

2.28 ISDP Commands

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

2.28.1 isdp run

This command enables ISDP on the switch.

Default Enabled

Format `isdp run`

Mode Global Config

2.28.1.1 no isdp run

This command disables ISDP on the switch.

Format `no isdp run`

Mode Global Config

2.28.2 isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default 180 seconds

Format `isdp holdtime <10-255>`

Mode Global Config

2.28.3 isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default 30 seconds

Format `isdp timer <5-254>`

Mode Global Config

2.28.4 isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default Enabled
Format `isdp advertise-v2`
Mode Global Config

2.28.4.1 no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format `no isdp advertise-v2`
Mode Global Config

2.28.5 isdp enabl

This command enables ISDP on the interface.

Default Enabled
Format `isdp enable`
Mode Interface Config

Note: ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command 2.28.1 “isdp run” on page 2 - 141.

2.28.5.1 no isdp enable

This command disables ISDP on the interface.

Format `no isdp enable`
Mode Interface Config

2.28.6 clear isdp counters

This command clears ISDP counters.

Format `clear isdp counters`
Mode Privileged EXEC

2.28.7 clear isdp table

This command clears entries in the ISDP table.

Format `clear isdp table`
Mode Privileged EXEC

2.28.8 show isdp

This command displays global ISDP settings.

Format `show isdp`

Mode Privileged EXEC

Term	*Definition*
Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
ISDPv2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	Indicates the Device ID format capability of the device. • `serialNumber` indicates that the device uses a serial number as the format for its Device ID. • `macAddress` indicates that the device uses a Layer 2 MAC address as the format for its Device ID. • `other` indicates that the device uses its platform-specific format as the format for its Device ID.
Device ID Format	Indicates the Device ID format of the device. • `serialNumber` indicates that the value is in the form of an ASCII string containing the device serial number. • `macAddress` indicates that the value is in the form of a Layer 2 MAC address. • `other` indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/ prepended with system name.

2.28.9 show isdp interface

This command displays ISDP settings for the specified interface.

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

Mode Privileged EXEC

Term	*Definition*
Mode	ISDP mode enabled/disabled status for the interface(s).

2.28.10 show isdp entry

This command displays ISDP entries. If the device id is specified, then only entries for that device are shown.

Format `show isdp entry {all | deviceid}`

Mode Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.

2.28.11 show isdp neighbors

This command displays the list of neighboring devices.

Format `show isdp neighbors [{<slot/port> | detail}]`

Mode Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	Displays when the entry was last modified.
Version	The software version that the neighbor is running.

Example: The following shows example CLI display output for the command.

```
(FASTPATH Switching) #show isdp neighbors detail

Device ID                      0001f45f1bc0
Address(es):
    IP Address:                10.27.7.57
Capability                     Router Trans Bridge Switch IGMP
Platform                       SecureStack C2
Interface                      0/48
Port ID                        ge.3.14
Holdtime                       131
Advertisement Version          2
Entry last changed time        0 days 00:01:59
Version :                      05.00.56
```

2.28.12 show isdp traffic

This command displays ISDP statistics.

Format `show isdp traffic`

Mode Privileged EXEC

Term	*Definition*
ISDP Packets Received	Total number of ISDP packets received
ISDP Packets Transmitted	Total number of ISDP packets transmitted
ISDPv1 Packets Received	Total number of ISDPv1 packets received
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted
ISDPv2 Packets Received	Total number of ISDPv2 packets received
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted
ISDP Bad Header	Number of packets received with a bad header
ISDP Checksum Error	Number of packets received with a checksum error
ISDP Transmission Failure	Number of packets which failed to transmit
ISDP Invalid Format	Number of invalid packets received
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

2.28.13 debug isdp packet

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Format `debug isdp packet [{receive | transmit}]`

Mode Privileged EXEC

2.28.13.1 no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format `no debug isdp packet [{receive | transmit}]`

Mode Privileged EXEC

2.29 Multicast Handling Commands

2.29.1 multicast (interface)

This command configures the port based multicast handling. The command defines the handling for port specific unregistered multicast addresses. The default handling in FASTPATH is that such packets are flooded (argument ‘default’). The user can change the behaviour that such packets are dropped (argument ‘none’). The flooding mode is set per port. It can be applied to either individual physical ports or to a port-channel.

Format `multicast flood {default | none}`

Mode Interface Config

2.29.2 show port multicast

This command displays the port based multicast handling. The commands displays for a specified interface or all interfaces the multicast flooding settings. The displayed fields are

- the interface
- the multicast flooding, indicating whether a packet with unregistered multicast address should be flooded or not (yes/no).

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

Mode Privileged Exec

2.29.3 multicast (VLAN)

This command configures the VLAN based multicast handling. The command defines the handling for VLAN based unregistered multicast addresses. The default handling in FASTPATH is that such packets are flooded (argument 'default'). The user can change the behaviour that such packets are dropped (argument 'none'). The flooding mode is set per VLAN, the VLAN ID range is 1-4093. If a created VLAN is deleted again, the flooding mode is reset to default.

Format **multicast** *<1-4093>* **flood** *{default | none}*

Mode VLAN Config

2.29.4 show vlan multicast

This command displays the VLAN based multicast handling. The command displays for a specified VLAN ID (range is 1-4093) or all created VLANs (inclusive default VLAN) the multicast flooding settings. The displayed fields are

- the VLAN Identifier (VID) associated with each VLAN
- the VLAN type (default, static or dynamic)
- the multicast flooding, indicating whether a packet with unregistered multicast address should be flooded or not (yes/no).

Format **show vlan multicast** *{ <1 - 4093> | all}*

Mode Privileged Exec

2.29.5 set igmp proxy-report interfacemode

This command enables sending of IGMP reports to the specified interface. The reports are sent for all locally subscribed multicast groups. This command is similar to set igmp mrouter interfacemode command, but multicast traffic will not be forwarded to the interface by default. It don't exist a separate "show" command, the setting may be seen in "show running-config".

Format **set igmp proxy-report interfacemode**

Mode Interface Config

2.29.5.1 no set igmp proxy-report interfacemode

This command disables sending of IGMP reports to the specified interface..

Format **no set igmp proxy-report interfacemode**

Mode Interface Config

2.30 Port Bridging Commands

2.30.1 L2-port-bridge

This command configures layer2 port bridging. L2 port bridging is a feature that allows a packet to be transmitted in egress direction through the same port it was received on.

Format `L2-port-bridge`

Mode Interface Config

2.30.1.1 no L2-port-bridge

This command resets L2 port bridging..

Format `no L2-port-bridge`

Mode Interface Config

2.30.2 show port L2-port-bridge

This command displays the L2 port bridge setting. The command displays for a specified interface or all interfaces the settings. The displayed fields are

- the interface
- enabled/disabled L2 port bridge

Format `show port L2-port-bridge` *{<slot/port> | all}*

Mode Priviledged Exec

Chapter 3

Quality of Service Commands

3. Quality of Service Commands

This chapter describes the Quality of Service (QoS) commands available in the FASTPATH CLI.

The QoS Commands chapter contains the following sections:

- 3.1 “Class of Service Commands” on page 3 - 2
- 3.2 “Differentiated Services Commands” on page 3 - 8
- 3.3 “DiffServ Class Commands” on page 3 - 9
- 3.4 “DiffServ Policy Commands” on page 3 - 16
- 3.5 “DiffServ Service Commands” on page 3 - 20
- 3.6 “DiffServ Show Commands” on page 3 - 21
- 3.7 “MAC Access Control List Commands” on page 3 - 27
- 3.8 “IP Access Control List Commands” on page 3 - 30
- 3.9 “IPv6 Access Control List Commands” on page 3 - 36
- 3.10 “Auto-Voice over IP Commands” on page 3 - 39
- 3.11 “iSCSI Optimization Commands” on page 3 - 40

Note: The commands in this chapter are in one of two 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.

3.1 Class of Service 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 “Voice VLAN Commands” on page 2 - 33.

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}*

Modes
- 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 “Voice VLAN Commands” on page 2 - 33.

Format **show classofservice dot1p-mapping** *[<slot/port>]*

Mode Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
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.

Term	*Definition*
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.

Term	*Definition*
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

Term	*Definition*
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

Term	*Definition*
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.

Term	*Definition*
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.

3.1.12 show protection-group

This command lists the protection groups and port egress masks. All or specified protection groups or port egress masks (for all or a specified interface) can be displayed. The protection groups are listed with the interface members, the egress masks are listed related to the calculation type (user specified, related to the protection group or '--' for default).

Format
`show protection-group` *`<0..63>`*
`show protection-group all`
`show protection-group mask` *`<slot/port`*
`show protection-group mask all`

Mode Privileged EXEC

3.1.13 protection-group (configure)

This command adds a protection group and/or a name associated to a group. The addition of a protection group has no effect as long as no members are included (interface). Optional a name can be assigned to a protection group with parameter ‘name’ when adding the group or for an already active group. The length of the name is restricted to 15 characters.

Format **protection-group** *<0..63>*
protection-group *<0..63>* **name** *<name>*

Mode Global Config

3.1.13.1 no protection-group (configure)

This command deletes a protection group and/or a name associated to a group. If deleting a protection group all members of this group are deleted too. The name can be deleted by using the ‘no’ command with the parameter ‘name’ (the protection group remains active then). The length of the name is restricted to 15 characters.

Format **no protection-group** *<0..63>*
no protection-group *<0..63>* **name** *<name>*

Mode Global Config

3.1.14 protection-group (interface)

This command includes/excludes interfaces to/from a protection group or sets an egress-mask for an interface.

If an interface is member in a protection group it may sent packets to interfaces which are not member of any group (unprotected) and to interfaces in the same group, but not to interfaces in another group. An egress-mask is calculated based on the protection-groups containing for each interface (bit 0 for first interface) a bit, indicating that it is allowed (1) or prohibited (0) to forward to this interface. The calculated egress-mask can be displayed by “show protection-group mask” below.

The calculated egress-mask may be overridden by setting directly this mask (use parameter “mask”).

For a LAG the minimal egress mask over all member interfaces (either calculated for protection-groups or directly set) is used (<mask-member-1> & … & <mask-member-N>).

Format **protection-group** *{<0..63> | mask <mask>}*

Mode Interface Config

3.1.14.1 no protection-group (interface)

The command deletes an interface to a protection group or deletes an egress port mask. The command deletes an egress mask for an interface if specifying the keyword ‘mask’.

Format **no protection-group** **{***<0..63> | mask <mask>}*

Mode Interface Config

3.1.15 clear protection-group

This command deletes all existing protection groups (inclusive the membership of ports to the protection groups). An explicit defined egress mask (see above) is not deleted.

Format	`clear protection-group`
Mode	Priviledged Exec

3.2 Differentiated Services 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
   a. Creating and deleting classes.
   b. Defining match criteria for a class.
2. Policy
   a. Creating and deleting policies
   b. Associating classes with a policy
   c. Defining policy statements for a policy/class combination
3. Service
   a. 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.

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.This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

Note: The optional keywords `[{ipv4 | ipv6}]` specify the Layer 3 protocol for this class. If not specified, this parameter defaults to `'ipv4'`. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported.

Note: The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the `[{ipv4 | ipv6}]` keyword specified.

Format **class-map match-all** *<class-map-name>* [{ipv4 | ipv6}]

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.

Default none

Format **class-map rename** *<class-map-name> <new-class-map-name>*

Mode Global Config

3.3.3 match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The *<ethertype>* value is specified as one of the following keywords: **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, **rarp** or as a custom ethertype value in the range of 0x0600-0xFFFF.

Note: This command is not available on the Broadcom 5630x platform.

Format **match ethertype** *{<keyword> | custom <0x0600-0xFFFF>}*

Mode Class-Map Config
Ipv6-Class-Map Config

3.3.4 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
Ipv6-Class-Map Config

3.3.5 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.

Default none

Format **match class-map** *<refclassname>*

Mode Class-Map Config
Ipv6-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.

3.3.5.1 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
Ipv6-Class-Map Config

3.3.6 match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

Note: This command is not available on the Broadcom 5630x platform.

Default none

Format **match cos** *<0-7>*

Mode Class-Map Config
Ipv6-Class-Map Config

3.3.7 match secondary-cos

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7..

Note: This command is supported on the following platforms:

- BCM56314
- BCM56504
- BCM56214
- BCM56224

Default	none
Format	**match secondary-cos** *<0-7>*
Mode	Class-Map Config Ipv6-Class-Map Config

3.3.8 match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The <macaddr> parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The <macmask**>** parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Note: This command is not available on the Broadcom 5630x platform.

Default	none
Format	**match destination-address mac** *<macaddr> <macmask>*
Mode	Class-Map Config Ipv6-Class-Map Config

3.3.9 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. The *<ipmask>* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default	none
Format	**match dstip** *<ipaddr> <ipmask>*
Mode	Class-Map Config

3.3.10 match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

Default	none
Format	**match dstip6** *<destination-ipv6-prefix/prefix-length>*
Mode	Ipv6-Class-Map Config

3.3.11 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 Ipv6-Class-Map Config

3.3.12 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 Ipv6-Class-Map Config

3.3.13 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

3.3.14 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

3.3.15 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 Ipv6-Class-Map Config

3.3.16 match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The <address> parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers

separated by colons (e.g., 00:11:22:dd:ee:ff). The <macmask> parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Note: This command is not available on the Broadcom 5630x platform.

Default	none
Format	**match source-address mac** *<address> <macmask>*
Mode	Class-Map Config Ipv6-Class-Map Config

3.3.17 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

3.3.18 match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Default	none
Format	**match srci**p6 <source-ipv6-prefix/prefix-length>
Mode	Ipv6-Class-Map Config

3.3.19 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 Ipv6-Class-Map Config

3.3.20 match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 1 to 4095.

Note: This command is not available on the Broadcom 5630x platform.

Default	none
Format	**match vlan** *<1-4095>*
Mode	Class-Map Config Ipv6-Class-Map Config

3.3.21 match secondary-vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN tagged packet). The secondary VLAN ID is an integer from 1 to 4095.

Note: This command is not available on the Broadcom 5630x platform.

Default	none
Format	**match secondary-vlan** *<1-4095>*
Mode	Class-Map Config Ipv6-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), Mirror, Police, Redirect

3.4.3 mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Note: This command is not available on the Broadcom 5630x platform.

Format	**mirror** *<slot/port>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

3.4.4 redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Note: This command is not available on the Broadcom 5630x platform.

Format	**redirect** *<slot/port>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mirror

3.4.5 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

3.4.6 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

3.4.6.1 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

3.4.7 mark cos

This command marks all packets for the associated traffic stream with the specified class of service (CoS) 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

3.4.8 mark cos-as-sec-cos

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking Cos as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format	**mark-cos-as-sec-cos**
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

Example: The following shows an example of the command.

```
(switch) (Config-policy-classmap)#mark cos-as-sec-cos
```

3.4.9 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

3.4.10 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.

Note: This command may not be used on IPv6 classes. IPv6 does not have a precedence field.

Format	**mark ip-precedence** *<0-7>*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

3.4.11 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)

3.4.12 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

3.4.12.1 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

3.4.13 policy-map rename

This command changes the name of a DiffServ policy. The *<policyname> i*s 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:

Term	*Definition*
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.
L3 Proto	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
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:

Term	*Definition*
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

Term	*Definition*
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.

Term	Definition
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:

Term	Definition
Policy Name	The name of this policy.
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)::

Term	Definition
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 Color Mode	The current setting for the color mode. Policing uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome.
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.

Term	*Definition*
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.
Exceed Action	The action taken on traffic that exceeds settings that the network administrator specifies.
Exceed Color Mode	The current setting for the color of exceeding traffic that the user may optionally specify.
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 CoS as Secondary CoS	The secondary 802.1p priority value (second/inner VLAN tag. Same as CoS (802.1p) marking, but the dot1p value used for remarking is picked from the dot1p value in the secondary (i.e. inner) tag of a double-tagged packet.
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.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. This field does not display on Broadcom 5630x platforms.
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.
Peak Rate	Guarantees a committed rate for transmission, but also transmits excess traffic bursts up to a user-specified peak rate, with the understanding that a downstream network element (such as the next hop's policer) might drop this excess traffic. Traffic is held in queue until it is transmitted or dropped (per type of queue depth management.) Peak rate shaping can be configured for the outgoing transmission stream for an AP traffic class (although average rate shaping could also be used.)
Peak Burst Size	(PBS). The network administrator can set the PBS as a means to limit the damage expedited forwarding traffic could inflict on other traffic (e.g., a token bucket rate limiter) Traffic that exceeds this limit is discarded.
Policing Style	The style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. This field does not display on Broadcom 5630x platforms.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Term	Definition
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.

Example: The following shows example CLI display output including the mark-cos-as-sec-cos option specified in the policy action.

```
(Broadcom FASTPATH Routing) #show policy-map p1
```

```
Policy Name..................................... p1
Policy Type..................................... In
Class Name...................................... c1
Mark CoS as Secondary CoS....................... Yes
```

Example: The following shows example CLI display output including the mark-cos-as-sec-cos action used in the policing (simple-police, police-single-rate, police two-rate) command.

```
(Broadcom FASTPATH Routing) #show policy-map p2
Policy Name..................... p2
Policy Type..................... In
Class Name...................... c2
Policing Style.................. Police Two Rate
Committed Rate.................. 1
Committed Burst Size............ 1
Peak Rate....................... 1
Peak Burst Size................. 1
Conform Action.................. Mark CoS as Secondary CoS
Exceed Action................... Mark CoS as Secondary CoS
Non-Conform Action.............. Mark CoS as Secondary CoS
Conform Color Mode.............. Blind
Exceed Color Mode............... Blind
```

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

Term	*Definition*
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 a forward slash.
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

Term	*Definition*
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):

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
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

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
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:

Term	*Definition*
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):

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
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 Commands

This section describes the commands you use to configure MAC Access Control List (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 can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- For the Broadcom 5630x platform, 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} (MAC ACL)

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: For BCM5630x and BCM5650x based systems, assign-queue, redirect, and mirror 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 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.

For the Broadcom 5650x platform, the *mirror* parameter allows the traffic matching this rule to be copied to the specified *<slot/port>*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *<slot/port>*. The *assign-queue* and *redirect* parameters are only valid for a **permit** rule.

Note: The *mirror* and *redirect* parameters are not available on the Broadcom 5630x platform.

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>]] [{mirror | redirect} <slot/port>]*

Mode Mac-Access-List Config

3.7.4 mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by *<name>* to an interface, or associates it with a VLAN ID, 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 VLAN keyword is only valid in the 'Global Config' mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

Note: You should be aware that the **<**out**>** option may or may not be available, depending on the platform.

Format **mac access-group** *<name> [vlan <vlan-id>]* **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-group** *<name> [vlan <vlan-id>]* **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

Term	*Definition*
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.
Mirror Interface	On Broadcom 5650x platforms, the slot/port to which packets matching this rule are copied.
Redirect Interface	On Broadcom 5650x platforms, the slot/port to which packets matching this rule are forwarded.

3.8 IP Access Control List Commands

This section describes the commands you use to configure IP Access Control List (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 hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- On Broadcom 5630x platforms, 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 2 describes the parameters for the **access-list** command.

IP Standard ACL:

Format **access-list** *<1-99> {deny | permit} {every | <srcip> <srcmask>} [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>]*

Mode Global Config

IP Extended ACL:

Format **access-list** *<100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask>[{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq {<portkey>| <0-65535>}] [precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>]*

Mode Global Config

Table 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:*** For 5630x and 5650x-based systems, assign-queue, redirect, and mirror 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.
[{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.
[{mirror | redirect} <slot/port>]	For Broadcom 5650x platforms, specifies the mirror or redirect interface which is the slot/port to which packets matching this rule are copied or forwarded, respectively. The *mirror* and *redirect* parameters are not available on the Broadcom 5630x platform.

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-list

This command creates an extended IP Access Control List (ACL) identified by <*name*>, consisting of classification fields defined for the IP header of an IPv4 frame. The <*name*> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Note: The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format **ip access-list** *<name>*
Mode Global Config

3.8.2.1 no ip access-list

This command deletes the IP ACL identified by <name> from the system.

Format **no ip access-list** *<name>*
Mode Global Config

3.8.3 ip access-list rename

This command changes the name of an IP Access Control List (ACL). The <*name*> parameter is the names of an existing IP ACL. The <new*name*> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails is an IP ACL by the name <new*name*> already exists.

Format **ip access-list rename** *<name> <newname>*
Mode Global Config

3.8.4 {deny | permit} (IP ACL)

This command creates a new rule for the current IP 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 an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and re-specified.

Note: An implicit 'deny all' IP rule always terminates the access list.

Note: The *mirror* parameter allows the traffic matching this rule to be copied to the specified *<slot/port>*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *<slot/port>*. The *assign-queue* and *redirect* parameters are only valid for a **permit** rule.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified 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 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.

Format *{deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask>[{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq {<portkey>| <0-65535>}] [precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>]*

Mode Ipv4-Access-List Config

3.8.5 ip access-group

This command either attaches a specific IP ACL identified by <accesslistnumber> to an interface or associates with a VLAN ID in a given direction. The parameter <name> is the name of the Access Control List.

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.

Note: You should be aware that the <out> option may or may not be available, depending on the platform.

Default none

Format **ip access-group** *<accesslistnumber> <name> [vlan <vlan-id>]* **<in | out>***[sequence <1-4294967295>]*

Modes
- Interface Config
- Global Config

3.8.5.1 no ip access-group

This command removes a specified IP ACL from an interface.

Default none

Format **no ip access-group** *<accesslistnumber> [vlan <vlan-id>]* **in**

Mode
- Interface Config
- Global Config

3.8.6 acl-trapflags

This command enables the ACL trap mode.

Default disabled

Format **acl-trapflags**

Mode Global Config

3.8.6.1 no acl-trapflags

This command disables the ACL trap mode.

Format **no acl-trapflags**

Mode Global Config

3.8.7 show acl-traptimer

This command displays the time interval for generating ACL traps. A trap is generated if a ACL rule applies for an incoming packet.

Format **show acl-traptimer**

Mode Privileged EXEC

3.8.8 acl-traptimer

This command sets the time interval for generating ACL traps. An ACL trap is generated if ACL trap generation is enabled and an ACL rule applies for an incoming packet. The generation is checked for a specified time interval. The time interval value indicates seconds.

Default 300

Format **acl-traptimer** *<30-600>*

Mode Global Config

3.8.8.1 no acl-traptimer

This command sets the time interval for generating ACL traps. An ACL trap is generated if ACL trap generation is enabled and an ACL rule applies for an incoming packet. The generation is checked for a specified time interval. The time interval value indicates seconds.

Format **no acl-traptimer**

Mode Global Config

3.8.9 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.

Term	*Definition*
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.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.

3.8.10 show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction.

Format **show access-lists interface** *<slot/port>* **in**

Mode Privileged EXEC

Term	*Definition*
ACL Type	Type of access list (IP, IPv6, or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.

Term	Definition
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).

3.9 IPv6 Access Control List Commands

This section describes the commands you use to configure IPv6 Access Control List (ACL) settings. IPv6 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 IPv6 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 IPv6 ACL is hardware dependent.

3.9.1 ipv6 access-list

This command creates an IPv6 Access Control List (ACL) identified by *<name>*, consisting of classification fields defined for the IP header of an IPv6 frame. The *<name>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

Note: The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format **ipv6 access-list** *<name>*

Mode Global Config

3.9.1.1 no ipv6 access-list

This command deletes the IPv6 ACL identified by *<name>* from the system.

Format **no ipv6 access-list** *<name>*

Mode Global Config

3.9.2 ipv6 access-list rename

This command changes the name of an IPv6 ACL. The *<name>* parameter is the name of an existing IPv6 ACL. The *<newname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name *<newname>* already exists.

Format	**ipv6 access-list rename** *<name> <newname>*
Mode	Global Config

3.9.3 {deny | permit} (IPv6)

This command creates a new rule for the current IPv6 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 an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

Note: An implicit 'deny all' IPv6 rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the *'every'* keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified 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 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.

For the Broadcom 5650x platform, the *mirror* parameter allows the traffic matching this rule to be copied to the specified *<slot/port>*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *<slot/port>*. The *assign-queue* and *redirect* parameters are only valid for a **permit** rule.

Note: The *mirror* and *redirect* parameters are not available on the Broadcom 5630x platform.

Format	*{deny | permit} {every | {log} [assign-queue <queue-id>] [{mirror | redirect} <slot/port>]*
Mode	IPv6-Access-List Config

3.9.4 ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by <name> to an interface or associates with a VLAN ID in a given direction. The <name> parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 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 specifiedIPv6 access list replaces the currently attached IPv6 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 `vlan` keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

Note: You should be aware that the <`out`> option may or may not be available, depending on the platform.

Format **`ipv6 traffic-filter <name>`** *`[vlan <vlan-id>]`* **`in`***`[sequence <1-4294967295>]`*

Modes
- Global Config
- Interface Config

3.9.4.1 no ipv6 traffic-filter

This command removes an IPv6 ACL identified by <`name`> from the interface(s) in a given direction.

Format **`no ipv6 traffic-filter <name>`** *`[vlan <vlan-id>]`* **`in`** *`[sequence <1-4294967295>]`*

Modes
- Global Config
- Interface Config

3.9.5 show ipv6 access-lists

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the *`[name]`* parameter to identify a specific IPv6 ACL to display.

Format **`show ipv6 access-lists`** *`[name]`*

Mode Privileged EXEC

Term	*Definition*
Rule Number	The ordered rule number identifier defined within the IPv6 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 L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.

3.10 Auto-Voice over IP Commands

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

3.10.1 auto-voip all

Use this command to enable VoIP Profile on the interfaces of the switch.

Default disabled
Format **`auto-voip all`**
Mode Global Config

3.10.1.1 no auto-voip all

Use this command to disable VoIP Profile on the interfaces of the switch.

Format **`no auto-voip all`**
Mode Global Config

3.10.2 auto-voip

Use this command to enable VoIP Profile on the interface.

Default disabled
Format **`auto-voip`**
Mode Interface Config

3.10.2.1 no auto-voip

Use this command to disable VoIP Profile on the interface.

Format **`no auto-voip all`**
Mode Interface Config

3.10.3 show auto-voip

Use this command to display the VoIP Profile settings on the interface or interfaces of the switch.

Format **`show auto-voip interface`** *{<slot/port>|all}*

Mode Privileged EXEC

Field	*Description*
AutoVoIP Mode	The Auto VoIP mode on the interface.
Traffic Class	The CoS Queue or Traffic Class to which all VoIP traffic is mapped to. This is not configurable and defaults to the highest CoS queue available in the system for data traffic.

3.11 iSCSI Optimization Commands

This section describes commands you use to monitor iSCSI sessions and prioritize iSCSI packets. iSCSI Optimzation provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establich iSCSI sessoins and connections. Data from these exchanges is ues to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port baesd on these rules.

3.11.1 iscsi aging time

This command sets the aging time for iSCSI sessions. Behavior when changing aging time:

- When aging time is increased, current sessions will be timed out according to the new value.
- When aging time is decreased, any sessions that have been dormant for a time exceeding the new setting will be immediately deleted from the table. All other sessions will continue to be monitored against the new time out value.

Default `10 minutes`

Format **`iscsi aging time`** *`time`*

Mode Global Config

Parameter	*Description*
time	The number of minutes a session must be inactive prior to its removal. Range: 1-43,200.

Example: The following example sets the aging time for iSCSI sessions to 100 minutes.

```
(switch)(config)#iscsi aging time 100
```

3.11.1.1 no iscsi aging time

Use the `no` form of the command to reset the aging time value to the default value.

Format `no iscsi aging time`

Mode Global Config

3.11.2 iscsi cos

This command sets the quality of service profile that will be applied to iSCSI flows. iSCSI flows are assigned by default to the highest VPT/DSCP mapped to the highest queue not used for stack management. The user should also take care of configuring the relevant Class of Service parameters for the queue in order to complete the setting.

Setting the VPT/DSCP sets the QoS profile which determines the egress queue to which the frame is mapped. The switch default setting for egress queues scheduling is Weighted Round Robin (WRR).

You may complete the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes via the Class of Service settings. Depending on the platform, these choices may include strict priority for the queue used for iSCSI traffic. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic may get starved. In WRR the queue to which the flow is assigned to can be set to get the required percentage.

Format **iscsi cos** {**vpt** *vpt* | **dscp** *dscp*} [**remark**]
Mode Global Config

Parameter	*Description*
vpt/dscp	The VLAN Priority Tag or DSCP to assign iSCSI session packets.
remark	Mark the iSCSI frames with the configured VPT/DSCP when egressing the switch.

Example: The following example sets the quality of service profile that will be applied to iSCSI flows.

```
(switch)(config)#iscsi cos vpt 5 remark
```

no iscsi cos

Use the `no` form of the command to return to the default.

Format `no iscsi cos`
Mode Global Config

3.11.3 iscsi enable

This command globally enables iSCSI awareness.

Default `disabled`
Format `iscsi enable`
Mode Global Config

Example: The following example enables iSCSI awareness.

```
(switch)(config)#iscsi enable
```

3.11.3.1 no iscsi enable

This command disables iSCSI awareness. When you use the **`no iscsi enable`** command, iSCSI resources will be released.

Format `no iscsi enable`
Mode Global Config

3.11.4 iscsi target port

This command configures an iSCSI target port and, optionally, a target system's IP address and IQN name. When working with private iSCSI ports (not IANA-assigned ports 3260/860), it is recommended to specify the target IP

address as well, so that the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, and the destination IP is the target's IP address. This way the CPU will not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these un-reserved ports.

When a port is already defined and not bound to an IP address, and you want to bind it to an IP address, you should first remove it by using the `no` form of the command and then add it again, this time together with the relevant IP address.

Target names are only for display when using the **show iscsi** command. These names are not used to match with the iSCSI session information acquired by snooping.

A maximum of 16 TCP ports can be configured either bound to IP or not.

Default iSCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target.

Format `iscsi target port` *`tcp-port-1`* `[`*`tcp-port-2...tcp-port-16`*`] [address` *`ip-address`*`] [name` *`targetname`*`]`

Mode Global Config

Parameter	*Description*
tcp-port-n	TCP port number or list of TCP port numbers on which the iSCSI target listens to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.
ip-address	IP address of the iSCSI target. When the no form of this command is used, and the tcp port to be deleted is one bound to a specific IP address, the address field must be present.
targetname	iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSNS or from sendTargets response. The initiator must present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection.

Example: The following example configures TCP Port 49154 to target IP address 172.16.1.20.

```
(switch)(config)#iscsi target port 49154 address 172.16.1.20
```

no iscsi target port

Use the `no` form of the command to delete an iSCSI target port, address, and name.

3.11.5 show iscsi

This command displays the iSCSI settings.

Format `show iscsi`

Mode Privileged EXEC

Example: The following are examples of the commands used for iSCSI.

Example #1: Show iSCSI (Default Configuration)

```
(switch)#show iscsi
iSCSI disabled
iSCSI vpt is 5, remark
Session aging time: 10 min
Maximum number of sessions is 192
```

```
-----------------------------------------
iSCSI Targets and TCP ports:
-----------------------------------------
TCP Port  Target IP Address   Name
860       Not Configured      Not Configured
3260      Not Configured      Not Configured
```

Example #2: Enable iSCSI.

```
(switch)#configure
(switch)(config)#iscsi enable
```

Example #3: Show iSCSI (After Enable)

The following configuration detects iSCSI sessions and connections established using TCP ports 3260 or 860. Packets sent on detected iSCSI TCP connections are assigned to traffic class 2 (see the CoS configuration shown below). Since remark is enabled, the packets are marked with IEEE 802.1p priority to 5 before transmission.

```
(switch)#show iscsi
iscsi enabled
iSCSI vpt is 5, remark
Session aging time: 10 min
Maximum number of sessions is 192
-----------------------------------------
iSCSI Targets and TCP ports:
-----------------------------------------
TCP Port  Target IP Address   Name
860       Not Configured      Not Configured
3260      Not Configured      Not Configured

(switch)#show classofservice dot1p-mapping
User Priority    Traffic Class
-------------    -------------
       0                1
       1                0
       2                0
       3                1
       4                2
       5                2
       6                3
       6                3
```

3.11.6 show iscsi sessions

This command displays the iSCSI sessions.

Default	`If not specified, sessions are displayed in short mode (not detailed).`
Format	`show iscsi sessions [detailed]`
Mode	Privileged EXEC

Example: The following example displays the iSCSI sessions.

```
(switch) # show iscsi sessions
Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
-----------------------------------------------------------
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
ISID: 11
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
```

```
ISID: 222
------------------------------------------------------------
Target: iqn.103-1.com.storage-vendor:sn.43338.
storage.tape:sys1.xyz
Session 3:
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
Session 4:
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
------------------------------------------------------------


(switch)# show iscsi sessions detailed
Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
------------------------------------------------------------
Session 1:

Initiator: iqn.1992-04.com.os
vendor.plan9:cdrom.12.storage:sys1.xyz
------------------------------------------------------------
Time started: 17-Jul-2008 10:04:50
Time for aging out: 10 min
ISID: 11

Initiator Initiator Target Target
IP address TCP port IP address IP port
172.16.1.3 49154 172.16.1.20 30001
172.16.1.4 49155 172.16.1.21 30001
172.16.1.5 49156 172.16.1.22 30001

Session 2:
------------------------------------------------------------
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
Time started: 17-Aug-2008  21:04:50
Time for aging out: 2 min
ISID: 22
Initiator Initiator Target Target
IP address TCP port IP address IP port
172.16.1.30 49200 172.16.1.20 30001
172.16.1.30 49201 172.16.1.21 30001
```

Routing Commands

4. Routing Commands

This chapter describes the routing commands available in the FASTPATH CLI.

The IPv4 Routing and Multicast options are not available on all board variants, please contact your local Kontron representative for additional information.

The Routing Commands chapter contains the following sections:

- 4.1 “Address Resolution Protocol Commands” on page 4 - 2
- 4.2 “IP Routing Commands” on page 4 - 7
- 4.3 “Router Discovery Protocol Commands” on page 4 - 15
- 4.4 “Virtual LAN Routing Commands” on page 4 - 18
- 4.5 “Virtual Router Redundancy Protocol Commands” on page 4 - 20
- 4.6 “DHCP and BOOTP Relay Commands” on page 4 - 27
- 4.7 “IP Helper Commands” on page 4 - 28
- 4.8 “Open Shortest Path First Commands” on page 4 - 35
- 4.9 “Routing Information Protocol Commands” on page 4 - 66
- 4.10 “ICMP Throttling Commands” on page 4 - 72

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.

4.1 Address Resolution Protocol Commands

This section describes the commands you use to configure Address Resolution Protocol (ARP) and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

4.1.1 arp

This command creates an ARP entry. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device.

The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format	**arp** *ipaddress macaddr*
Mode	Global Config

4.1.1.1 no arp

This command deletes an ARP entry. The value for *arpentry* is the IP address of the interface. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device.

Format **no arp** *ipaddress macaddr*
Mode Global Config

4.1.2 ip proxy-arp

This command enables proxy ARP on a router interface or range of interfaces. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default enabled
Format **ip proxy-arp**
Mode Interface Config

4.1.2.1 no ip proxy-arp

This command disables proxy ARP on a router interface.

Format **no ip proxy-arp**
Mode Interface Config

4.1.3 arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

Format **arp cachesize** *platform specific integer value*
Mode Global Config

4.1.3.1 no arp cachesize

This command configures the default ARP cache size.

Format **no arp cachesize**
Mode Global Config

4.1.4 arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out.

Default disabled
Format **arp dynamicrenew**
Mode Global Config

4.1.4.1 no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format **no arp dynamicrenew**
Mode Global Config

4.1.5 arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format **arp purge** *ipaddr*
Mode Privileged EXEC

4.1.6 arp resptime

This command configures the ARP request response timeout.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for *seconds* is between 1-10 seconds.

Default 1
Format **arp resptime** *seconds*
Mode Global Config

4.1.6.1 no arp resptime

This command configures the default ARP request response timeout.

Format **no arp resptime**
Mode Global Config

4.1.7 arp retries

This command configures the ARP count of maximum request for retries.

The value for *retries* is an integer, which represents the maximum number of request for retries. The range for *retries* is an integer between 0-10 retries.

Default 4
Format **arp retries** *retries*
Mode Global Config

4.1.7.1 no arp retries

This command configures the default ARP count of maximum request for retries.

Format **no arp retries**
Mode Global Config

4.1.8 arp timeout

This command configures the ARP entry ageout time.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for *seconds* is between 15-21600 seconds.

Default 1200

Format **arp timeout** *seconds*

Mode Global Config

4.1.8.1 no arp timeout

This command configures the default ARP entry ageout time.

Format **no arp timeout**

Mode Global Config

4.1.9 clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the *gateway* keyword is specified, the dynamic entries of type gateway are purged as well.

Format **clear arp-cache** *[gateway]*

Mode Privileged EXEC

4.1.10 clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, **ping** from the remote system to the DUT. Issue the **show arp switch** command to see the ARP entries. Then issue the **clear arp-switch** command and check the **show arp switch** entries. There will be no more arp entries.

Format **clear arp-switch**

Mode Privileged EXEC

4.1.11 show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the **show arp** results in conjunction with the **show arp switch** results.

Format **show arp**

Mode Privileged EXEC

Term	*Definition*
Age Time (seconds)	The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.

Term	Definition
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Term	Definition
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing slot/port associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

4.1.12 show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format `show arp brief`

Mode Privileged EXEC

Term	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This value is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

4.1.13 show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format `show arp switch`

Mode Privileged EXEC

Term	Definition
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing slot/port associated with the device's ARP entry.

4.2 IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

4.2.1 routing

This command enables IPv4 and IPv6 routing for an interface or range of interfaces. You can view the current value for this function with the **`show ip brief`** command. The value is labeled as "Routing Mode."

Default disabled

Format **`routing`**

Mode Interface Config

4.2.1.1 no routing

This command disables routing for an interface.

You can view the current value for this function with the **`show ip brief`** command. The value is labeled as "Routing Mode."

Format **`no routing`**

Mode Interface Config

4.2.2 ip routing

This command enables the IP Router Admin Mode for the master switch.

Format **`ip routing`**

Mode Global Config

4.2.2.1 no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format **`no ip routing`**

Mode Global Config

4.2.3 ip address

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface.The value for *`ipaddr`* is the IP address of the interface. The value for *`subnetmask`* is a 4-digit dotted-decimal number which represents the subnet mask of the

interface. The subnet mask must have contiguous ones and be no longer than 30 bits, for example 255.255.255.0. This command adds the label IP address in **show ip interface**.

Format **ip address** *ipaddr subnetmask [secondary]*

Mode Interface Config

4.2.3.1 no ip address

This command deletes an IP address from an interface. The value for *ipaddr* is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for *subnetmask* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command **no ip address**.

Format **no ip address** *[{ipaddr subnetmask [secondary]}]*

Mode Interface Config

4.2.4 ip route

This command configures a static route. The *ipaddr* parameter is a valid IP address, and *subnetmask* is a valid subnet mask. The *nexthopip* parameter is a valid IP address of the next hop router. Specifying Null0 as nexthop parameter adds a static reject route. The optional *preference* parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Default preference—1

Format **ip route** *ipaddr subnetmask [nexthopip | Null0] [preference]*

Mode Global Config

4.2.4.1 no ip route

This command deletes a single next hop to a destination static route. If you use the *nexthopip* parameter, the next hop is deleted. If you use the *preference* value, the preference value of the static route is reset to its default.

Format **no ip route** *ipaddr subnetmask [{nexthopip [preference] | Null0}]*

Mode Global Config

4.2.5 ip route default

This command configures the default route. The value for *nexthopip* is a valid IP address of the next hop router. The *preference* is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default preference—1

Format **ip route default** *nexthopip [preference]*

Mode Global Config

4.2.5.1 no ip route default

This command deletes all configured default routes. If the optional *nexthopip* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Format **no ip route default** *[{nexthopip | preference}]*

Mode Global Config

4.2.6 ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The **ip route** and **ip route default** commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **ip route distance** command.

Default 1

Format **ip route distance** *<1-255>*

Mode Global Config

4.2.6.1 no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format **no ip route distance**

Mode Global Config

4.2.7 ip netdirbcast

This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default disabled

Format **ip netdirbcast**

Mode Interface Config

4.2.7.1 no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Format	**`no ip netdirbcast`**
Mode	Interface Config

4.2.8 ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. FASTPATH software currently does not fragment IP packets.

- Packets forwarded in hardware ignore the IP MTU.
- Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the ip mtu command.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the **`ip ospf mtu-ignore`** command.)

Note: The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (See 2.1.8 “mtu” on page 2 - 5) must take into account the size of the Ethernet header.

Default	1500 bytes
Format	**`ip mtu`** *`<68-1500>`*
Mode	Interface Config

4.2.8.1 no ip mtu

This command resets the ip mtu to the default value.

Format	**`no ip mtu`** *`mtu`*
Mode	Interface Config

4.2.9 encapsulation

This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be *`ethernet`* or *`snap`*.

Default	ethernet
Format	**`encapsulation`** *`{ethernet	snap}`*
Mode	Interface Config

Note: Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

4.2.10 show ip brief

This command displays all the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.

Format `show ip brief`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. *Burst-interval* is from 0 to 2147483647 milliseconds. The default *burst-interval* is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.

Example: The following shows example CLI display output for the command.

```
(Switch) #show ip brief

Default Time to Live.......................... 64
Routing Mode.................................. Disabled
Maximum Next Hops............................. 4
Maximum Routes................................ 6000
ICMP Rate Limit Interval...................... 1000 msec
ICMP Rate Limit Burst Size.................... 100 messages
ICMP Echo Replies............................. Enabled
ICMP Redirects................................ Enabled
```

4.2.11 show ip interface

This command displays all pertinent information about the IP interface.

Format `show ip interface` *slot/port*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.

Term	Definition
Helper IP Address	The helper IP addresses configured by the "clear ip helper statistics" command.
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).

Example: The following shows example CLI display output for the command.

```
(switch)#show ip interface 0/2

Routing Interface Status..................... Down
Primary IP Address........................... 1.2.3.4/255.255.255.0
Secondary IP Address(es)..................... 21.2.3.4/255.255.255.0
.............................................. 22.2.3.4/255.255.255.0
Helper IP Address............................ 1.2.3.4
.............................................. 1.2.3.5
Routing Mode................................. Disable
Administrative Mode.......................... Enable
Forward Net Directed Broadcasts.............. Disable
Proxy ARP.................................... Enable
Local Proxy ARP.............................. Disable
Active State................................. Inactive
Link Speed Data Rate......................... Inactive
MAC Address.................................. 00:10:18:82:0C:68
Encapsulation Type........................... Ethernet
IP MTU....................................... 1500
Bandwidth.................................... 100000 kbps
Destination Unreachables..................... Enabled
ICMP Redirects............................... Enabled
```

4.2.12 show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

Format `show ip interface brief`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
MultiCast Fwd	The multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

4.2.13 show ip route

This command displays the routing table. The *ip-address* specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The *mask* specifies the subnet mask for the given *ip-address*. When you use the *longer-prefixes* keyword, the *ip-address* and *mask* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the *protocol* parameter to specify the protocol that installed the routes. The value for *protocol* can be *connected*, *ospf*, *rip* or *static*. Use the *all* parameter to display all routes including best and non-best routes. If you do not use the *all* parameter, the command only displays the best route.

Note: If you use the *connected* keyword for *protocol*, the *all* option is not available because there are no best or non-best connected routes.

Format **show ip route** *[{ip-address [protocol] | {ip-address mask [longer-prefixes] [protocol] | protocol} [all] | all}]*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The **show ip route** command displays the routing tables in the following format:

```
Code   IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface
```

The columns for the routing table display the following information:

Term	*Definition*
Code	The codes for the routing protocols that created the routes.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Term	Definition
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be • Days:Hours:Minutes if days > = 1 • Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2

C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2,   00h:00m:01s,  0/5
C 11.11.11.0/24 [0/1] directly connected,   0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
```

4.2.14 show ip route summary

Use this command to display the routing table summary. Use the optional *all* parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

Format **show ip route summary** *[all]*

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by BGP protocol.
OSPF Routes	Total number of routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Total Routes	Total number of routes in the routing table.

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show ip route summary

Connected Routes.............................1
Static Routes................................7
RIP Routes...................................0
BGP Routes...................................0
OSPF Routes..................................0
  Intra Area Routes..........................0
  Inter Area Routes..........................0
  External Type-1 Routes.....................0
  External Type-2 Routes.....................0
Reject Routes................................2
Total routes.................................8
```

4.2.15 show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format `show ip route preferences`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Local	The local route preference value.
Static	The static route preference value.
OSPF Intra	The OSPF Intra route preference value.
OSPF Inter	The OSPF Inter route preference value.
OSPF External	The OSPF External route preference value.
RIP	The RIP route preference value.
BGP4	The BGP-4 route preference value.

4.2.16 show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format `show ip stats`

Modes
- Privileged EXEC
- User EXEC

4.3 Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

4.3.1 ip irdp

This command enables Router Discovery on an interface or range of interfaces.

Default disabled

Format **`ip irdp`**

Mode Interface Config

4.3.1.1 no ip irdp

This command disables Router Discovery on an interface.

Format **`no ip irdp`**

Mode Interface Config

4.3.2 ip irdp address

This command configures the address that the interface uses to send the router discovery advertisements. The valid values for *`ipaddr`* are 224.0.0.1, which is the all-hosts IP multicast address, and 255.255.255.255, which is the limited broadcast address.

Default 224.0.0.1

Format **`ip irdp address`** *`ipaddr`*

Mode Interface Config

4.3.2.1 no ip irdp address

This command configures the default address used to advertise the router for the interface.

Format **`no ip irdp address`**

Mode Interface Config

4.3.3 ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of *`maxadvertinterval`* to 9000 seconds.

Default 3 * maxinterval

Format **`ip irdp holdtime`** *`maxadvertinterval-9000`*

Mode Interface Config

4.3.3.1 no ip irdp holdtime

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Format **`no ip irdp holdtime`**

Mode Interface Config

4.3.4 ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for maxadvertinterval is 4 to 1800 seconds.

Default 600

Format **`ip irdp maxadvertinterval`** *<4-1800>*

Mode Interface Config

4.3.4.1 no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format **`no ip irdp maxadvertinterval`**

Mode Interface Config

4.3.5 ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is three to the value of maxadvertinterval.

Default 0.75 * maxadvertinterval

Format **`ip irdp minadvertinterval`** *3-maxadvertinterval*

Mode Interface Config

4.3.5.1 no ip irdp minadvertinterval

This command sets the default minimum time to the default.

Format **`no ip irdp minadvertinterval`**

Mode Interface Config

4.3.6 ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.

Default 0

Format **`ip irdp preference`** *<-2147483648 to 2147483647>*

Mode Interface Config

4.3.6.1 no ip irdp preference

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Format **`no ip irdp preference`**

Mode Interface Config

4.3.7 show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

Format **show ip irdp** *{slot/port | all}*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The *slot/port* that matches the rest of the information in the row.
Ad Mode	The advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Dest Address	The destination IP address for router advertisements.
Max Int	The maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	The minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	The amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	The preference of the address as a default router address, relative to other router addresses on the same subnet.

4.4 Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

4.4.1 vlan routing

This command enables routing on a VLAN. The *vlanid* value has a range from 1 to 4093. The *[interface ID]* value has a range from 1 to 128. Typically, you will not supply the interface ID argument, and the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the slot/port for the VLAN routing interface. If you select an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface. For products that use text-based configuration, including the interface ID in the vlan routing command for the text configuration ensures that the slot/port for the VLAN interface stays the same across a restart. Keeping the slot/port the same ensures that the correct interface configuration is applied to each interface when the system restarts.

Format **vlan routing** *vlanid [interface ID]*

Mode VLAN Config

4.4.1.1 no vlan routing

This command deletes routing on a VLAN.

Format **no vlan routing** *vlanid*

Mode VLAN Config

Example: Example 1 shows the command specifying a vlanid value. The interface ID argument is not used.

```
(Switch)(Vlan)#vlan 14
(Switch)(Vlan)#vlan routing 14 ?
<cr>                    Press enter to execute the command.
<1-128>                 Enter interface ID
```

Typically, you press <**Enter**> without supplying the Interface ID value; the system automatically selects the interface ID.

Example: In Example 2, the command specifies interface ID 51 for VLAN 14 interface. The interface ID becomes the port number in the slot/port for the VLAN routing interface. In this example, slot/port is 4/51 for VLAN 14 interface.

```
(Switch)(Vlan)#vlan 14 51
(Switch)(Vlan)#
(Switch)#show ip vlan
MAC Address used by Routing VLANs:   00:11:88:59:47:36

           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  -------------  ---------------  ---------------
10       4/1            172.16.10.1      255.255.255.0
11       4/50           172.16.11.1      255.255.255.0
12       4/3            172.16.12.1      255.255.255.0
13       4/4            172.16.13.1      255.255.255.0
14       4/51           0.0.0.0          0.0.0.0  <--u/s/p is 4/51 for VLAN 14
interface
```

Example: In Example 3, you select an interface ID that is already in use. In this case, the CLI displays an error message and does not create the VLAN interface.

```
(Switch) #show ip vlan

MAC Address used by Routing VLANs:   00:11:88:59:47:36

           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  -------------  ---------------  ---------------
10       4/1            172.16.10.1      255.255.255.0
11       4/50           172.16.11.1      255.255.255.0
12       4/3            172.16.12.1      255.255.255.0
13       4/4            172.16.13.1      255.255.255.0
14       4/51           0.0.0.0          0.0.0.0

(Switch)#config

(Switch)(Config)#exit

(Switch)#vlan database

(Switch)(Vlan)#vlan 15

(Switch)(Vlan)#vlan routing 15 1

Interface ID 1 is already assigned to another interface
```

Example: The show running configuration command always lists the interface ID for each routing VLAN, as shown in Example 4 below.

```
(Switch) #show running-config
!Current Configuration:
```

```
!
!System Description "Alpha HELIX 56314 Development System - 48 GB, 4.24.10.4, VxWorks
6.5"
!System Software Version "4.24.10.4"
!System Up Time          "0 days 0 hrs 22 mins 19 secs"
!Additional Packages     None
!Current SNTP Synchronized Time: Not Synchronized
!
set prompt "02.08"
network protocol dhcp
vlan database
vlan 10-14
vlan routing 10 1
vlan routing 12 3
vlan routing 13 4
vlan routing 11 50
vlan routing 14 51
```

4.4.2 show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format **show ip vlan**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
MAC Address used by Routing VLANs	The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	The identifier of the VLAN.
Logical Interface	The logical slot/port associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.
Subnet Mask	The subnet mask that is associated with this VLAN.

4.5 Virtual Router Redundancy Protocol Commands

This section describes the commands you use to view and configure Virtual Router Redundancy Protocol (VRRP) and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

4.5.1 ip vrrp (Global Config)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router.

Default none

Format **ip vrrp**

Mode Global Config

4.5.1.1 no ip vrrp

Use this command in Global Config mode to disable the default administrative mode of VRRP on the router.

Format **no ip vrrp**
Mode Global Config

4.5.2 ip vrrp (Interface Config)

Use this command in Interface Config mode to create a virtual router associated with the interface or range of interfaces. The parameter *vrid* is the virtual router ID, which has an integer value range from 1 to 255.

Format **ip vrrp** *vrid*
Mode Interface Config

4.5.2.1 no ip vrrp

Use this command in Interface Config mode to delete the virtual router associated with the interface. The virtual Router ID, *vrid*, is an integer value that ranges from 1 to 255.

Format **no ip vrrp** *vrid*
Mode Interface Config

4.5.3 ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter *vrid* is the virtual router ID which has an integer value ranging from 1 to 255.

Default disabled
Format **ip vrrp** *vrid* **mode**
Mode Interface Config

4.5.3.1 no ip vrrp mode

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Format **no ip vrrp** *vrid* **mode**
Mode Interface Config

4.5.4 ip vrrp ip

This command sets the virtual router IP address value for an interface or range of interfaces. The value for *ipaddr* is the IP address which is to be configured on that interface for VRRP. The parameter *vrid* is the virtual router ID which has an integer value range from 1 to 255. You can use the optional *[secondary]* parameter to designate the IP address as a secondary IP address.

Default none
Format **ip vrrp** *vrid* **ip** *ipaddr [secondary]*
Mode Interface Config

4.5.4.1 no ip vrrp ip

Use this command in Interface Config mode to delete a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

Format **no ip vrrp** *vrid ipaddress secondary*

Mode Interface Config

4.5.5 ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface or range of interfaces. The parameter *{none | simple}* specifies the authorization type for virtual router configured on the specified interface. The parameter *[key]* is optional, it is only required when authorization type is simple text password. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Default no authorization

Format **ip vrrp** *vrid* **authentication** *{none | simple key}*

Mode Interface Config

4.5.5.1 no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface or range of interfaces.

Format **no ip vrrp** *vrid* **authentication**

Mode Interface Config

4.5.6 ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface or range of interfaces. The parameter *vrid* is the virtual router ID, which is an integer from 1 to 255.

Default enabled

Format **ip vrrp** *vrid* **preempt**

Mode Interface Config

4.5.6.1 no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface or range of interfaces.

Format **no ip vrrp** *vrid* **preempt**

Mode Interface Config

4.5.7 ip vrrp priority

This command sets the priority of a router within a VRRP group. It can be used to configure an interface or a range of interfaces. Higher values equal higher priority. The range is from 1 to 254. The parameter *vrid* is the virtual router ID, whose range is from 1 to 255.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the “address owner.” The priority of the address owner is always 255 so that the address owner is always master. If the master has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the master’s priority, the router will take over as master only if preempt mode is enabled.

Default 100 unless the router is the address owner, in which case its priority is automatically set to 255.

Format **ip vrrp** *vrid* **priority** *<1-254>*

Mode Interface Config

4.5.7.1 no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface or range of interfaces.

Format **no ip vrrp** *vrid* **priority**

Mode Interface Config

4.5.8 ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.

Default 1

Format **ip vrrp** *vrid* **timers advertise** *<1-255>*

Mode Interface Config

4.5.8.1 no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface or range of interfaces.

Format **no ip vrrp** *vrid* **timers advertise**

Mode Interface Config

4.5.9 ip vrrp track interface

Use this command to alter the priority of the VRRP router based on the availability of its interfaces. This command is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if the IP on that interface is up. Otherwise, the tracked interface is down. The command can be used to configure an interface or a range of interfaces.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the *priority* argument. When the interface is up for IP protocol, the priority will be incremented by the *priority* value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed interface. The default priority decrement is changed using the *priority* argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10.

Default priority: 10

Format **ip vrrp** *vrid* track interface *slot/port* [decrement priority]

Mode Interface Config

4.5.9.1 no ip vrrp track interface

Use this command to remove the interface or range of interfaces from the tracked list or to restore the priority decrement to its default.

Format **no ip vrrp** *vrid* track interface *slot/port* [decrement]

Mode Interface Config

4.5.10 ip vrrp track ip route

Use this command to track the route reachability on an interface or range of interfaces. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the *priority* argument. When the tracked route is added, the priority will be incremented by the same.

A VRRP configured interface can track more than one route. When a tracked route goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed route. By default no routes are tracked. If you specify just the route to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10. The default priority decrement is changed using the *priority* argument.

Default priority: 10

Format **ip vrrp** *vrid* track ip route *ip-address/prefix-length* [decrement *priority*]

Mode Interface Config

4.5.10.1 no ip vrrp track ip route

Use this command to remove the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, the priority should be incremented by the decrement value if the route is not reachable.

Format **no ip vrrp** *vrid* track interface *slot/port* [decrement]

Mode Interface Config

4.5.11 show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch.

Format **show ip vrrp interface stats** *slot/port vrid*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Uptime	The time that the virtual router has been up, in days, hours, minutes and seconds.

Term	Definition
Protocol	The protocol configured on the interface.
State Transitioned to Master	The total number of times virtual router state has changed to MASTER.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	The total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
Authentication Failure	The total number of VRRP packets received that don't pass the authentication check.
IP TTL errors	The total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.
Zero Priority Packets Received	The total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	The total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	The total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	The total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
Packet Length Errors	The total number of VRRP packets received with packet length less than length of VRRP header.

4.5.12 show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring. This command takes no options.

Format `show ip vrrp`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
VRRP Admin Mode	The administrative mode for VRRP functionality on the switch.
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with invalid VRID for this virtual router.

4.5.13 show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface. Use the output of the command to verify the track interface and track IP route configurations.

Format **show ip vrrp interface** *slot/port vrid*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
IP Address	The configured IP address for the Virtual router.
VMAC address	The VMAC address of the specified router.
Authentication type	The authentication type for the specific virtual router.
Priority	The priority value for the specific virtual router, taking into account any priority decrements for tracked interfaces or routes.
Configured Priority	The priority configured through the **ip vrrp vrid priority <*1-254*>** command.
Advertisement interval	The advertisement interval in seconds for the specific virtual router.
Pre-Empt Mode	The preemption mode configured on the specified virtual router.
Administrative Mode	The status (Enable or Disable) of the specific router.
State	The state (Master/backup) of the virtual router.

Example: The following shows example CLI display output for the command.

```
show ip vrrp interface <u/s/p> vrid

Primary IP Address.............................. 1.1.1.5
VMAC Address.................................... 00:00:5e:00:01:01
Authentication Type............................. None
Priority........................................ 80
  Configured priority........................... 100
Advertisement Interval (secs)................... 1
Pre-empt Mode................................... Enable
Administrative Mode............................. Enable
State........................................... Initialized

Track Interface          State          DecrementPriority
---------------         ------          ------------------

<0/1>                   down                 10

TrackRoute   (pfx/len)      State         DecrementPriority
------------------------   ------          ------------------
10.10.10.1/255.255.255.0    down               10
```

4.5.14 show ip vrrp interface brief

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format **show ip vrrp interface brief**

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Valid slot and port number separated by a forward slash.
VRID	The router ID of the virtual router.
IP Address	The virtual router IP address.
Mode	Indicates whether the virtual router is enabled or disabled.
State	The state (Master/backup) of the virtual router.

4.6 DHCP and BOOTP Relay Commands

This section describes the commands you use to configure BootP/DHCP Relay on the switch. A DHCP relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

4.6.1 bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Default disabled

Format **`bootpdhcprelay cidoptmode`**

Mode Global Config

4.6.1.1 no bootpdhcprelay cidoptmode

This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

Format **`no bootpdhcprelay cidoptmode`**

Mode Global Config

4.6.2 bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The *`hops`* parameter has a range of 1 to 16.

Default 4

Format **`bootpdhcprelay maxhopcount`** *`<1-16>`*

Mode Global Config

4.6.2.1 no bootpdhcprelay maxhopcount

This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

Format **`no bootpdhcprelay maxhopcount`**

Mode Global Config

4.6.3 bootpdhcprelay minwaittime

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field

of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

Default 0

Format **bootpdhcprelay minwaittime** *<0-100>*

Mode Global Config

4.6.3.1 no bootpdhcprelay minwaittime

This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

Format **no bootpdhcprelay minwaittime**

Mode Global Config

4.6.4 show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format **show bootpdhcprelay**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Server IP Address	The IP address for the BootP/DHCP Relay server.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.
Requests Received	The number or requests received.
Requests Relayed	The number of requests relayed.
Packets Discarded	The number of packets discarded.

4.7 IP Helper Commands

This section describes the commands to configure and monitor the IP Helper agent. IP Helper relays DHCP and other broadcast UDP packets from a local client to one or more servers which are not on the same network at the client.

The IP Helper feature provides a mechanism that allows a router to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications to reach servers on non-local subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

The network administrator can configure relay entries both globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). The network administrator may configure multiple relay entries for the same interface and UDP port, in which case the relay agent

relays matching packets to each server address. Interface configuration takes priority over global configuration. That is, if a packet's destination UDP port matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

The network administrator can configure discard relay entries, which direct the system to discard matching packets. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

In addition to configuring the server addresses, the network administrator also configures which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI as a convenience, but the network administrator can configure a relay entry with any UDP port number. The network administrator may configure relay entries that do not specify a destination UDP port. The relay agent relays assumes these entries match packets with the UDP destination ports listed in Table 1. This is the list of default ports.

Table 1: Default Ports - UDP Port Numbers Implied by Wildcard

Protocol	*UDP Port Number*
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

The system limits the number of relay entries to four times the maximum number of routing interfaces. The network administrator can allocate the relay entries as he likes. There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for a given {interface, UDP port} pair.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays to the client packets that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent checks if the interface is configured to relay the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent checks if there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed. Note that if the packet matches a discard relay entry on the ingress interface, then the packet is not forwarded, regardless of the global configuration.

The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF)
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.

- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

4.7.1 clear ip helper statistics

Use this command to reset to zero the statistics displayed in the **show ip helper statistics** command.

Format	`clear ip helper statistics`
Mode	Privileged EXEC

Example: The following shows an example of the command.

```
(switch) #clear ip helper statistics
```

4.7.2 ip helper-address (Global Config)

Use this command to configure the relay of certain UDP broadcast packets received on any interface. This command can be invoked multiple times, either to specify multiple server addresses for a given UDP port number or to specify multiple UDP port numbers handled by a specific server.

Default	No helper addresses are configured.
Format	**`ip helper-address`** *`server-address [dest-udp-port	dhcp	domain	isakmp	mobile-ip	nameserver	netbios-dgm	netbios-ns	ntp	pim-auto-rp	rip	tacacs	tftp	time]`*
Mode	Global Config

Parameter	*Description*
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
dest-udp-port	A destination UDP port number from 0 to 65535.
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • dhcp (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • ntp (port 123) • pim-auto-rp (port 496) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Example: To relay DHCP packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands:

```
(switch)#config
(switch)(config)#ip helper-address 10.1.1.1 dhcp
(switch)(config)#ip helper-address 10.1.2.1 dhcp
```

Example: To relay UDP packets received on any interface for all default ports to the server at 20.1.1.1, use the following commands:

```
(switch)#config
(switch)(config)#ip helper-address 20.1.1.1
```

4.7.2.1 no ip helper-address (Global Config)

Use the **no** form of the command to delete an IP helper entry. The command **no ip helper-address** with no arguments clears all global IP helper addresses.

Format **no ip helper-address** *[server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]*

Mode Global Config

4.7.3 ip helper-address (Interface Config)

Use this command to configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

Default No helper addresses are configured.

Format **ip helper-address** *{server-address | discard} [dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]*

Mode Interface Config

Parameter	*Description*
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be in a subnet on the interface where the relay entry is configured, and cannot be an IP address configured on any interface of the local router.
discard	Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.
dest-udp-port	A destination UDP port number from 0 to 65535.

Parameter	*Description*
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: • dhcp (port 67) • domain (port 53) • isakmp (port 500) • mobile-ip (port 434) • nameserver (port 42) • netbios-dgm (port 138) • netbios-ns (port 137) • ntp (port 123) • pim-auto-rp (port 496) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Example: To relay DHCP packets received on interface 0/2 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands:

```
(switch)#config
(switch)(config)#interface 0/2
(switch)(interface 0/2)#ip helper-address 192.168.10.1 dhcp
(switch)(interface 0/2)#ip helper-address 192.168.20.1 dhcp
```

Example: To relay both DHCP and DNS packets to 192.168.30.1, use the following commands:

```
(switch)#config
(switch)(config)#interface 0/2
(switch)(interface 0/2)#ip helper-address 192.168.30.1 dhcp
(switch)(interface 0/2)#ip helper-address 192.168.30.1 dns
```

Example: This command takes precedence over an ip helper-address command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than 0/2 and 0/17 to 192.168.40.1, relays DHCP and DNS packets received on 0/2 to 192.168.40.2, relays SNMP traps (port 162) received on interface 0/17 to 192.168.23.1, and drops DHCP packets received on 0/17:

```
(switch)#config
(switch)(config)#ip helper-address 192.168.40.1 dhcp
(switch)(config)#interface 0/2
(switch)(interface 0/2)#ip helper-address 192.168.40.2 dhcp
(switch)(interface 0/2)#ip helper-address 192.168.40.2 domain
(switch)(interface 0/2)#exit
(switch)(config)#interface 0/17
(switch)(interface 0/17)#ip helper-address 192.168.23.1 162
(switch)(interface 0/17)#ip helper-address discard dhcp
```

no ip helper-address (Interface Config)

Use this command to delete a relay entry on an interface. The no command with no arguments clears all helper addresses on the interface.

Format **no ip helper-address [server-address | discard][dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]**

Mode Interface Config

4.7.4 ip helper enable

Use this command to enable relay of UDP packets. This command can be used to temporarily disable IP helper without deleting all IP helper addresses. This command replaces the **bootpdhcprelay enable** command, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

Default disabled

Format **ip helper enable**

Mode Global Config

Example: The following shows an example of the command.

```
(switch)(config)#ip helper enable
```

4.7.4.1 no ip helper enable

Use the no form of this command to disable relay of all UDP packets.

Format **no ip helper enable**

Mode Global Config

4.7.5 show ip helper-address

Use this command to display the IP helper address configuration.

Format **show ip helper-address** [*slot/port*]

Mode Privileged EXEC

Parameter	*Description*
interface	The relay configuration is applied to packets that arrive on this interface. This field is set to any for global IP helper entries.
UDP Port	The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as any are applied to packets with the destination UDP ports listed in Table 4.
Discard	If Yes, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

Example: The following shows example CLI display output for the command.

```
(switch) #show ip helper-address

IP helper is enabled

Interface        UDP Port     Discard   Hit Count   Server Address
---------------  -----------  --------  ----------  ---------------
```

```
0/1             dhcp         No         10          10.100.1.254
                                                    10.100.2.254
0/17            any          Yes         2
                any dhcp     No          0          10.200.1.254
```

4.7.6 show ip helper statistics

Use this command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent.

Format `show ip helper statistics`

Mode Privileged EXEC

Parameter	*Description*
DHCP client messages received	The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL>1 and having valid source and destination IP addresses.
DHCP client messages relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP server messages received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP server messages relayed	The number of DHCP server messages relayed to a client.
UDP clients messages received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP clients messages relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.
DHCP message hop count exceeded max	The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with secs field below min	The number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with giaddr set to local address	The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurance.
Packets with expired TTL	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.

Example: The following shows example CLI display output for the command.

```
(switch)#show ip helper statistics

DHCP client messages received..................  8
DHCP client messages relayed...................  2
DHCP server messages received..................  2
DHCP server messages relayed...................  2
UDP client messages received...................  8
UDP client messages relayed....................  2
```

```
DHCP message hop count exceeded max..... 0
DHCP message with secs field below min..... 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL..... 0
Packets that matched a discard entry..... 0
```

4.8 Open Shortest Path First Commands

This section describes the commands you use to view and configure Open Shortest Path First (OSPF), which is a link-state routing protocol that you use to route traffic within a network.

4.8.1 router ospf

Use this command to enter Router OSPF mode.

Format **router ospf**

Mode Global Config

4.8.2 enable (OSPF)

This command resets the default administrative mode of OSPF in the router (active).

Default enabled

Format **enable**

Mode Router OSPF Config

4.8.2.1 no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

Format **no enable**

Mode Router OSPF Config

4.8.3 network area (OSPF)

Use this command to enable OSPFv2 on an interface and set its area ID if the IP address of an interface is covered by this network command.

Default disabled

Format **network** *ip-address wildcard-mask* **area** *area-id*

Mode Router OSPF Config

4.8.3.1 no network area (OSPF)

Use this command to disable the OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command.

Format **no network** *ip-address wildcard-mask* **area** *area-id*

Mode Router OSPF Config

4.8.4 ip ospf area

Use this command to enable OSPFv2 and set the area ID of an interface or range of interfaces. The area-id is an IP address formatted as a 4-digit dotted-decimal number or a decimal value in the range of <0-4294967295>. This command supersedes the effects of the **network area** command. It can also be used to configure the advertiseability of the secondary addresses on this interface into the OSPFv2 domain.

Default disabled

Format **ip ospf area area-id [secondaries none]**

Mode Interface Config

4.8.4.1 no ip ospf area

Use this command to disable OSPF on an interface or range of interfaces.

Format **no ip ospf area [secondaries none]**

Mode Interface Config

4.8.5 1583compatibility

This command enables OSPF 1583 compatibility.

Note: 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Default enabled

Format **1583compatibility**

Mode Router OSPF Config

4.8.5.1 no 1583compatibility

This command disables OSPF 1583 compatibility.

Format **no 1583compatibility**

Mode Router OSPF Config

4.8.6 area default-cost (OSPF)

This command configures the default cost for the stub area. You must specify the area ID and an integer value between 1-16777215.

Format **area** *areaid* **default-cost** *<1-16777215>*

Mode Router OSPF Config

4.8.7 area nssa (OSPF)

This command configures the specified areaid to function as an NSSA.

Format **area** *areaid* **nssa**

Mode Router OSPF Config

4.8.7.1 no area nssa

This command disables nssa from the specified area id.

Format **no area** *areaid* **nssa**

Mode Router OSPF Config

4.8.8 area nssa default-info-originate (OSPF)

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is ****. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Format **area** *areaid* **nssa default-info-originate** *[metric] [{comparable | non-comparable}]*

Mode Router OSPF Config

4.8.8.1 no area nssa default-info-originate (OSPF)

This command disables the default route advertised into the NSSA.

Format **no area** *areaid* **nssa default-info-originate** *[metric] [{comparable | non-comparable}]*

Mode Router OSPF Config

4.8.9 area nssa no-redistribute (OSPF)

This command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

Format **area** *areaid* **nssa no-redistribute**

Mode Router OSPF Config

4.8.9.1 no area nssa no-redistribute (OSPF)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format **no area** *areaid* **nssa no-redistribute**

Mode Router OSPF Config

4.8.10 area nssa no-summary (OSPF)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format **area** *areaid* **nssa no-summary**

Mode Router OSPF Config

4.8.10.1 no area nssa no-summary (OSPF)

This command disables nssa from the summary LSAs.

Format **no area** *areaid* **nssa no-summary**

Mode Router OSPF Config

4.8.11 area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. A value of *always* causes the router to assume the role of the translator the instant it becomes a border router and a value of *candidate* causes the router to participate in the translator election process when it attains border router status.

Format **area** *areaid* **nssa translator-role** *{always | candidate}*

Mode Router OSPF Config

4.8.11.1 no area nssa translator-role (OSPF)

This command disables the nssa translator role from the specified area id.

Format **no area** *areaid* **nssa translator-role** *{always | candidate}*

Mode Router OSPF Config

4.8.12 area nssa translator-stab-intv (OSPF)

This command configures the translator *stabilityinterval* of the NSSA. The *stabilityinterval* is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format **area** *areaid* **nssa translator-stab-intv** *stabilityinterval*

Mode Router OSPF Config

4.8.12.1 no area nssa translator-stab-intv (OSPF)

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format **no area** *areaid* **nssa translator-stab-intv** *stabilityinterval*

Mode Router OSPF Config

4.8.13 area range (OSPF)

This command creates a specified area range for a specified NSSA. The *ipaddr* is a valid IP address. The *subnetmask* is a valid subnet mask. The LSDB type must be specified by either *summarylink* or *nssaexternallink*, and the advertising of the area range can be allowed or suppressed.

Format **area** *areaid* **range** *ipaddr subnetmask {summarylink | nssaexternallink} [advertise | not-advertise]*

Mode Router OSPF Config

4.8.13.1 no area range

This command deletes a specified area range. The *ipaddr* is a valid IP address. The *subnetmask* is a valid subnet mask.

Format **no area** *areaid* **range** *ipaddr subnetmask*

Mode Router OSPF Config

4.8.14 area stub (OSPF)

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format **area** *areaid* **stub**

Mode Router OSPF Config

4.8.14.1 no area stub

This command deletes a stub area for the specified area ID.

Format **no area** *areaid* **stub**

Mode Router OSPF Config

4.8.15 area stub no-summary (OSPF)

This command configures the Summary LSA mode for the stub area identified by *areaid*. Use this command to prevent LSA Summaries from being sent.

Default disabled

Format **area** *areaid* **stub no-summary**

Mode Router OSPF Config

4.8.15.1 no area stub no-summary

This command configures the default Summary LSA mode for the stub area identified by *areaid*.

Format **no area** *areaid* **stub no-summary**

Mode Router OSPF Config

4.8.16 area virtual-link (OSPF)

This command creates the OSPF virtual interface for the specified *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format **area** *areaid* **virtual-link** *neighbor*

Mode Router OSPF Config

4.8.16.1 no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format **no area** *areaid* **virtual-link** *neighbor*

Mode Router OSPF Config

4.8.17 area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The value for *type* is either none, simple, or encrypt. The *[key]* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id in the range of 0 and 255 must be specified.The default value for authentication type is none. Neither the default password key nor the default key id are configured.

Default none

Format **area** *areaid* **virtual-link** *neighbor* **authentication** *{none | {simple key} | {encrypt key keyid}}*

Mode Router OSPF Config

4.8.17.1 no area virtual-link authentication

This command configures the default authentication type for the OSPF virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format **no area** *areaid* **virtual-link** *neighbor* **authentication**

Mode Router OSPF Config

4.8.18 area virtual-link dead-interval (OSPF)

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

Default 40

Format **area** *areaid* **virtual-link** *neighbor* **dead-interval** *seconds*

Mode Router OSPF Config

4.8.18.1 no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format **no area** *areaid* **virtual-link** *neighbor* **dead-interval**

Mode Router OSPF Config

4.8.19 area virtual-link hello-interval (OSPF)

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 1 to 65535.

Default 10

Format **area** *areaid* **virtual-link neighbor hello-interval <***1-65535***>**

Mode Router OSPF Config

4.8.19.1 no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by **areaid** and **neighbor**. The **neighbor** parameter is the Router ID of the neighbor.

Format **no area** *areaid* **virtual-link neighbor hello-interval**

Mode Router OSPF Config

4.8.20 area virtual-link retransmit-interval (OSPF)

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600.

Default 5

Format **area areaid virtual-link neighbor retransmit-interval seconds**

Mode Router OSPF Config

4.8.20.1 no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by **areaid** and **neighbor**. The **neighbor** parameter is the Router ID of the neighbor.

Format **no area areaid virtual-link neighbor retransmit-interval**

Mode Router OSPF Config

4.8.21 area virtual-link transmit-delay (OSPF)

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by **areaid** and **neighbor**. The **neighbor** parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600 (1 hour).

Default 1

Format **area areaid virtual-link neighbor transmit-delay seconds**

Mode Router OSPF Config

4.8.21.1 no area virtual-link transmit-delay

This command resets the default transmit delay for the OSPF virtual interface to the default value.

Format **no area areaid virtual-link neighbor transmit-delay**

Mode Router OSPF Config

4.8.22 auto-cost (OSPF)

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the **auto-cost reference bandwidth** and **bandwidth** commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where interface bandwidth is defined by the **bandwidth** command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the **auto-cost** command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1-4294967 Mbps. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

Default 100Mbps

Format **auto-cost reference-bandwidth <***1 to 4294967***>**

Mode Router OSPF Config

4.8.22.1 no auto-cost reference-bandwidth (OSPF)

Use this command to set the reference bandwidth to the default value.

Format **no auto-cost reference-bandwidth**

Mode Router OSPF Config

4.8.23 bandwidth

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the **auto-cost** command. For the purpose of the OSPF link cost calculation, use the bandwidth command to specify the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface.

Default actual interface bandwidth

Format **bandwidth** *<1-10000000>*

Mode Interface Config

4.8.23.1 no bandwidth

Use this command to set the interface or range of interfaces bandwidth to its default value.

Format **no bandwidth**

Mode Interface Config

4.8.24 capability opaque

Use this command to enable Opaque Capability on the Router. The information contained in Opaque LSAs may be used directly by OSPF or indirectly by an application wishing to distribute information throughout the OSPF domain. FASTPATH supports the storing and flooding of Opaque LSAs of different scopes. The default value of enabled applies to OSPFv2, but not to OSPFv3 because OSPFv3 does not use opaque LSAs. The default value of enabled means that OSPFv2 will forward opaque LSAs by default. If you want to upgrade from a previous release, where the default was disabled, opaque LSA forwarding will be enabled. If you want to disable opaque LSA forwarding, then you should enter the command no capability opaque in OSPF router configuration mode after the software upgrade.

Default	enabled
Format	**`capability opaque`**
Mode	Router Config

4.8.24.1 no capability opaque

Use this command to disable opaque capability on the router.

Format	**`no capability opaque`**
Mode	Router Config

4.8.25 clear ip ospf

Use this command to disable and re-enable OSPF.

Format	`clear ip ospf`
Mode	Privileged EXEC

4.8.26 clear ip ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format	`clear ip ospf configuration`
Mode	Privileged EXEC

4.8.27 clear ip ospf counters

Use this command to reset global and interface statistics.

Format	`clear ip ospf counters`
Mode	Privileged EXEC

4.8.28 clear ip ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter [*neighbor-id*].

Format `clear ip ospf neighbor [neighbor-id]`

Mode Privileged EXEC

4.8.29 clear ip ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter [*slot/port*]. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [*neighbor-id*].

Format `clear ip ospf neighbor interface [slot/port] [neighbor-id]`

Mode Privileged EXEC

4.8.30 clear ip ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

Format `clear ip ospf redistribution`

Mode Privileged EXEC

4.8.31 default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Default
- metric—unspecified
- type—2

Format **`default-information originate`** *`[always] [metric <0-16777214>] [metric-type {1 | 2}]`*

Mode Router OSPF Config

4.8.31.1 no default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Format **`no default-information originate`** *`[metric] [metric-type]`*

Mode Router OSPF Config

4.8.32 default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format **`default-metric`** *`<1-16777214>`*

Mode Router OSPF Config

4.8.32.1 no default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format **`no default-metric`**

Mode Router OSPF Config

4.8.33 distance ospf (OSPF)

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be *intra, inter*, or *external*. All the external type routes are given the same preference value. The range of `preference` value is 1 to 255.

Default 110

Format **distance ospf** *{intra-area <1-255> | inter-area <1-255> | external <1-255>}*

Mode Router OSPF Config

4.8.33.1 no distance ospf

This command sets the default route preference value of OSPF routes in the router. The type of OSPF can be intra, inter, or external. All the external type routes are given the same preference value.

Format **no distance ospf** *{intra-area | inter-area | external}*

Mode Router OSPF Config

4.8.34 distribute-list out (OSPF)

Use this command to specify the access list to filter routes received from the source protocol.

Format **distribute-list** *<1-199>* **out** *{rip | bgp | static | connected}*

Mode Router OSPF Config

4.8.34.1 no distribute-list out

Use this command to specify the access list to filter routes received from the source protocol.

Format **no distribute-list** *<1-199>* **out** *{rip | bgp | static | connected}*

Mode Router OSPF Config

4.8.35 exit-overflow-interval (OSPF)

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave overflow state until restarted. The range for seconds is 0 to 2147483647 seconds.

Default 0

Format **exit-overflow-interval** *seconds*

Mode Router OSPF Config

4.8.35.1 no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format **no exit-overflow-interval**

Mode Router OSPF Config

4.8.36 external-lsdb-limit (OSPF)

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for limit is -1 to 2147483647.

Default -1

Format **external-lsdb-limit** *limit*

Mode Router OSPF Config

4.8.36.1 no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format **no external-lsdb-limit**

Mode Router OSPF Config

4.8.37 ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface or range of interfaces. The value of `type` is either none, simple or encrypt. The key is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. If the type is encrypt a `keyid` in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID. There is no default value for this command.

Format **ip ospf authentication** *{none | {simple key} | {encrypt key keyid}}*

Mode Interface Config

4.8.37.1 no ip ospf authentication

This command sets the default OSPF Authentication Type for the specified interface or range of interfaces.

Format **no ip ospf authentication**

Mode Interface Config

4.8.38 ip ospf cost

This command configures the cost on an OSPF interface or range of interfaces. The *cost* parameter has a range of 1 to 65535.

Default 10

Format `ip ospf cost <1-65535>`
Mode Interface Config

4.8.38.1 no ip ospf cost

This command configures the default cost on an OSPF interface or range of interfaces.

Format `no ip ospf cost`
Mode Interface Config

4.8.39 ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface or range of interfaces. The value for `seconds` is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range in seconds from 1 to 2147483647.

Note: Effective with FASTPATH 4.4.4 and later, valid values range in seconds from 1 to 65535.

Default 40
Format `ip ospf dead-interval seconds`
Mode Interface Config

4.8.39.1 no ip ospf dead-interval

This command sets the default OSPF dead interval for the specified interface or range of interfaces.

Format `no ip ospf dead-interval`
Mode Interface Config

4.8.40 ip ospf hello-interval

This command sets the OSPF hello interval for the specified interface or range of interfaces. The value for seconds is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network. Valid values range from 1 to 65535.

Default 10
Format `ip ospf hello-interval seconds`
Mode Interface Config

4.8.40.1 no ip ospf hello-interval

This command sets the default OSPF hello interval for the specified interface or range of interfaces.

Format `no ip ospf hello-interval`
Mode Interface Config

4.8.41 ip ospf network

Use this command to configure OSPF to treat an interface or range of interfaces as a point-to-point rather than broadcast interface. The **broadcast** option sets the OSPF network type to broadcast. The **point-to-point** option sets the OSPF network type to point-to-point. OSPF treats interfaces as broadcast interfaces by default. (Loopback interfaces have a special loopback network type, which cannot be changed.) When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

Default broadcast

Format **ip ospf network {broadcast|point-to-point}**

Mode Interface Config

4.8.41.1 no ip ospf network

Use this command to return the OSPF network type to the default.

Format **no ip ospf network**

Mode Interface Config

4.8.42 ip ospf priority

This command sets the OSPF priority for the specified router interface or range of interfaces. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default 1, which is the highest router priority

Format **ip ospf priority** *<0-255>*

Mode Interface Config

4.8.42.1 no ip ospf priority

This command sets the default OSPF priority for the specified router interface or range of interfaces.

Format **no ip ospf priority**

Mode Interface Config

4.8.43 ip ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface or range of interfaces. The retransmit interval is specified in seconds. The value for `seconds` is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

Default 5

Format **ip ospf retransmit-interval** *<0-3600>*

Mode Interface Config

4.8.43.1 no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface or range of interfaces.

Format **no ip ospf retransmit-interval**
Mode Interface Config

4.8.44 ip ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface or range of interfaces. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for *seconds* range from 1 to 3600 (1 hour).

Default 1
Format **ip ospf transmit-delay** *<1-3600>*
Mode Interface Config

4.8.44.1 no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface or range of interfaces.

Format **no ip ospf transmit-delay**
Mode Interface Config

4.8.45 ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface or range of interfaces. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default enabled
Format **ip ospf mtu-ignore**
Mode Interface Config

4.8.45.1 no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format **no ip ospf mtu-ignore**
Mode Interface Config

4.8.46 router-id (OSPF)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The `ipaddress` is a configured value.

Format **router-id** *ipaddress*
Mode Router OSPF Config

4.8.47 redistribute (OSPF)

This command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

Default
- metric—unspecified
- type—2
- tag—0

Format **redistribute** *{rip | bgp | static | connected} [metric <0-16777214>] [metric-type {1 | 2}] [tag <0-4294967295>] [subnets]*

Mode Router OSPF Config

4.8.47.1 no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/ routers.

Format **no redistribute** *{rip | bgp | static | connected} [metric] [metric-type] [tag] [subnets]*

Mode Router OSPF Config

4.8.48 maximum-paths (OSPF)

This command sets the number of paths that OSPF can report for a given destination where *maxpaths* is platform dependent.

Default 4

Format **maximum-paths** *maxpaths*

Mode Router OSPF Config

4.8.48.1 no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format **no maximum-paths**

Mode Router OSPF Config

4.8.49 passive-interface default (OSPF)

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF will not form adjacencies over a passive interface.

Default disabled

Format **passive-interface default**

Mode Router OSPF Config

4.8.49.1 no passive-interface default

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Format `no passive-interface default`

Mode Router OSPF Config

4.8.50 passive-interface (OSPF)

Use this command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Default disabled

Format `passive-interface {slot/port | tunnel tunnel-id}`

Mode Router OSPF Config

4.8.50.1 no passive-interface

Use this command to set the interface or tunnel as non-passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Format `no passive-interface {slot/port | tunnel tunnel-id}`

Mode Router OSPF Config

4.8.51 timers spf

Use this command to configure the SPF delay time and hold time. The valid range for both parameters is 0-65535 seconds.

Default
- delay-time—5
- hold-time—10

Format `timers spf delay-time hold-time`

Mode Router OSPF Config

4.8.52 trapflags (OSPF)

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group's specific trapflags to enable or disable, are listed in Table 2.

Table 2: Trapflags Groups

Group	*Flags*
errors	• authentication-failure • bad-packet • config-error • virt-authentication-failure • virt-bad-packet • virt-config-error

Group	Flags
if-rx	ir-rx-packet
lsa	• lsa-maxage • lsa-originate
overflow	• lsdb-overflow • lsdb-approaching-overflow
retransmit	• packets • virt-packets
rtb	• rtb-entry-info
state-change	• if-state-change • neighbor-state-change • virtif-state-change • virtneighbor-state-change

- To enable the individual flag, enter the **`group name`** followed by that particular flag.
- To enable all the flags in that group, give the group name followed by **`all`**.
- To enable all the flags, give the command as **`trapflags all`**.

Default disabled

Format

```
trapflags {
all |
errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
if-rx {all | if-rx-packet} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
rtb {all, rtb-entry-info} |
state-change {all | if-state-change | neighbor-state-change | virtif-
state-
change | virtneighbor-state-change}
}
```

Mode Router OSPF Config

4.8.52.1 no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the **`group name`** followed by that particular flag.
- To disable all the flags in that group, give the group name followed by **`all`**.
- To disable all the flags, give the command as **`trapflags all`**.

Format

```
no trapflags {
all |
errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
if-rx {all | if-rx-packet} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
rtb {all, rtb-entry-info} |
state-change {all | if-state-change | neighbor-state-change | virtif-
state-
change | virtneighbor-state-change}
}
```

Mode Router OSPF Config

4.8.53 show ip ospf

This command displays information relevant to the OSPF router.

Format `show ip ospf`

Mode Privileged EXEC

Note: Some of the information below displays only if you enable OSPF and configure certain features.

Term	*Definition*
Router ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
ASBR Mode	Indicates whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).
RFC 1583 Compatibility	Indicates whether 1583 compatibility is enabled or disabled. This is a configured value.
External LSDB Limit	The maximum number of non-default AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
Spf Delay Time	The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.
Spf Hold Time	The number of seconds between two consecutive spf calculations.
Opaque Capability	Shows whether the router is capable of sending Opaque LSAs. This is a configured value.
Autocost Ref BW	Shows the value of auto-cost reference bandwidth configured on the router.
ABR Status	Shows whether the router is an OSPF Area Border Router.

Term	*Definition*
ASBR Status	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. The router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocols. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router	When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
External LSDB Overflow	When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
AS_OPAQUE LSA Count	Shows the number of AS Opaque LSAs in the link-state database.
AS_OPAQUE LSA Checksum	Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
Retransmit List Entries	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
Maximum Number of Retransmit Entries	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
Retransmit Entries High Water Mark	The highest number of LSAs that have been waiting for acknowledgment.
External LSDB Limit	The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Default Metric	Default value for redistributed routes.
Default Passive Setting	Shows whether the interfaces are passive by default.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not.
Always	Shows whether default routes are always advertised.
Metric	The metric of the routes being redistributed. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Number of Active Areas	The number of active OSPF areas. An “active” OSPF area is an area with at least one interface up.
AutoCost Ref BW	Shows the value of auto-cost reference bandwidth configured on the router.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.

Term	*Definition*
Redistributing	This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.
Source	The source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.
Tag	The decimal value attached to each external route.
Subnets	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
Distribute-List	The access list used to filter redistributed routes.

Example: The following shows example CLI display output for the command.

```
(alpha2) #show ip ospf

Router ID.....................................2.2.2.2
OSPF Admin Mode...............................Disable
RFC 1583 Compatibility........................Enable
External LSDB Limit...........................No Limit
Exit Overflow Interval........................0
Spf Delay Time................................5
Spf Hold Time.................................10
Opaque Capability.............................Disable
AutoCost Ref BW...............................100 Mbps
Default Passive Setting.......................Disabled
Maximum Paths.................................4
Default Metric................................Not configured

Default Route Advertise.......................Disabled
Always........................................FALSE
Metric........................................Not configured
Metric Type...................................External Type 2


Number of Active Areas.......................... 3 (3 normal, 0 stub, 0 nssa)
ABR Status....................................Disable
ASBR Status...................................Disable
Stub Router...................................FALSE
External LSDB Overflow........................FALSE
External LSA Count............................0
External LSA Checksum.........................0
AS_OPAQUE LSA Count...........................0
AS_OPAQUE LSA Checksum........................0
LSAs Originated...............................0
LSAs Received.................................0
LSA Count.....................................0
Maximum Number of LSAs........................18200
LSA High Water Mark...........................0
Retransmit List Entries....................... 9078
Maximum Number of Retransmit Entries........... 72800
Retransmit Entries High Water Mark............. 72849
```

show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.

Format `show ip ospf abr`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
Type	The type of the route to the destination. It can be either: • intra — Intra-area route • inter — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

4.8.54 show ip ospf area

This command displays information about the area. The `areaid` identifies the OSPF area that is being displayed.

Format `show ip ospf area` *areaid*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
AreaID	The area id of the requested OSPF area.
External Routing	A number representing the external routing capabilities for this area.
Spf Runs	The number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.
Area LSA Checksum	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
Import Summary LSAs	Shows whether to import summary LSAs.
OSPF Stub Metric Value	The metric value of the stub area. This field displays only if the area is a configured as a stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA:

Term	*Definition*
Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.

Term	Definition
Default Information Originate	Shows whether to advertise a default route into the NSSA.
Default Metric	The metric value for the default route advertised into the NSSA.
Default Metric Type	The metric type for the default route advertised into the NSSA.
Translator Role	The NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	The amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

4.8.55 show ip ospf asbr

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR). This command takes no options.

Format `show ip ospf asbr`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Type	The type of the route to the destination. It can be one of the following values: intra — Intra-area route inter — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

4.8.56 show ip ospf database

This command displays information about the link state database when OSPF is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional *areaid* parameter to display database information about a specific area. Use the optional parameters to specify the type of link state advertisements to display.

Parameter	Description
asbr-summary	Use *asbr-summary* to show the autonomous system boundary router (ASBR) summary LSAs.
external	Use *external* to display the external LSAs.
network	Use *network* to display the network LSAs.
nssa-external	Use *nssa-external* to display NSSA external LSAs.
opaque-area	Use *opaque-area* to display area opaque LSAs.
opaque-as	Use *opaque-as* to display AS opaque LSAs.
opaque-link	Use *opaque-link* to display link opaque LSAs.
router	Use *router* to display router LSAs.

Parameter	Description
summary	Use *summary* to show the LSA database summary information.
lsid	Use *lsid* to specify the link state ID (LSID). The value of *lsid* can be an IP address or an integer in the range of 0-4294967295.
adv-router	Use *adv-router* to show the LSAs that are restricted by the advertising router.
self-originate	Use *self-originate* to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled

The information below is only displayed if OSPF is enabled.

Format **show ip ospf** *[areaid]* **database** *[{database-summary | [{asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary}] [lsid] [{adv-router [ipaddr] | self-originate}]}]*

Mode
- Privileged EXEC
- User EXEC

For each link-type and area, the following information is displayed:

Term	Definition
Link Id	A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Adv Router	The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.
Age	A number representing the age of the link state advertisement in seconds.
Sequence	A number that represents which LSA is more recent.
Checksum	The total number LSA checksum.
Options	This is an integer. It indicates that the LSA receives special handling during routing calculations.
Rtr Opt	Router Options are valid for router links only.

4.8.57 show ip ospf database database-summary

Use this command to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database.

Format **show ip ospf database database-summary**

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Router	Total number of router LSAs in the OSPF link state database.
Network	Total number of network LSAs in the OSPF link state database.
Summary Net	Total number of summary network LSAs in the database.
Summary ASBR	Number of summary ASBR LSAs in the database.
Type-7 Ext	Total number of Type-7 external LSAs in the database.
Self-Originated Type-7	Total number of self originated AS external LSAs in the OSPFv3 link state database.

Term	Definition
Opaque Link	Number of opaque link LSAs in the database.
Opaque Area	Number of opaque area LSAs in the database.
Subtotal	Number of entries for the identified area.
Opaque AS	Number of opaque AS LSAs in the database.
Total	Number of entries for all areas.

4.8.58 show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

Format `show ip ospf interface {slot/port | loopback loopback-id}`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
IP Address	The IP address for the specified interface.
Subnet Mask	A mask of the network and host portion of the IP address for the OSPF interface.
Secondary IP Address(es)	The secondary IP addresses if any are configured on the interface.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area ID for the specified interface.
OSPF Network Type	The type of network on this interface that the OSPF is running on.
Router Priority	A number representing the OSPF Priority for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.
Transmit Delay	A number representing the OSPF Transmit Delay Interval for the specified interface.
Authentication Type	The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.
Metric Cost	The cost of the OSPF interface.
Passive Status	Shows whether the interface is passive or not.
OSPF MTU-ignore	Indicates whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.

The information below will only be displayed if OSPF is enabled.

Term	Definition
OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value *broadcast*. The OSPF Interface Type will be 'broadcast'.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.

Term	Definition
Number of Link Events	The number of link events.
Local Link LSAs	The number of Link Local Opaque LSAs in the link-state database.
Local Link LSA Checksum	The sum of LS Checksums of Link Local Opaque LSAs in the link-state database.

Example: The following shows example CLI display output for the command when the OSPF Admin Mode is disabled.

```
(Broadcom FASTPATH Routing) >show ip ospf interface 0/1

IP Address..................................... 0.0.0.0
Subnet Mask.................................... 0.0.0.0
Secondary IP Address(es)....................
OSPF Admin Mode................................ Disable
OSPF Area ID................................... 0.0.0.0
OSPF Network Type.............................. Broadcast
Router Priority................................ 1
Retransmit Interval............................ 5
Hello Interval................................. 10
Dead Interval.................................. 40
LSA Ack Interval............................... 1
Transmit Delay................................. 1
Authentication Type............................ None
Metric Cost.................................... 1  (computed)
Passive Status................................. Non-passive interface
OSPF Mtu-ignore................................ Disable

OSPF is not enabled on this interface.

(Broadcom FASTPATH Routing) #
```

4.8.59 show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format **`show ip ospf interface brief`**

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Valid slot and port number separated by a forward slash.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area Id for the specified interface.
Router Priority	A number representing the OSPF Priority for the specified interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Retransmit Delay Interval	A number representing the OSPF Transit Delay for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.

4.8.60 show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

Format **show ip ospf interface stats** *slot/port*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
OSPF Area ID	The area id of this OSPF interface.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
AS Border Router Count	The total number of Autonomous System border routers reachable within this area.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IP Address	The IP address associated with this OSPF interface.
OSPF Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
Sent Packets	The number of OSPF packets transmitted on the interface.
Received Packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Source Not On Local Subnet	The number of received packets discarded because the source IP address is not within a subnet configured on a local interface. ***Note:*** This field only applies to OSPFv2.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
Wrong Authentication Type	The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface. ***Note:*** This field only applies to OSPFv2.
Authentication Failure	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. ***Note:*** This field only applies to OSPFv2.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. ***Note:*** Does not apply to Hellos.

Term	Definition
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Table 3 lists the number of OSPF packets of each type sent and received on the interface.

Table 3: Type of OSPF Packets Sent and Received on the Interface

Packet Type	Sent	Received
Hello	6960	6960
Database Description	3	3
LS Request	1	1
LS Update	141	42
LS Acknowledgment	40	135

4.8.61 show ip ospf neighbor

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays. The *ip-address* is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Format **show ip ospf neighbor [***interface slot/port***] [ip-address]**

Modes
- Privileged EXEC
- User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

Term	Definition
Router ID	The 4-digit dotted-decimal number of the neighbor router.
Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
IP Address	The IP address of the neighbor.
Interface	The interface of the local router in slot/port format.

Term	Definition
State	The state of the neighboring routers. Possible values are: • Down - initial state of the neighbor conversation - no recent information has been received from the neighbor. • Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. • Init - an Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. • 2 way - communication between the two routers is bidirectional. • Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number. • Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor. • Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

If you specify an IP address for the neighbor router, the following fields display:

Term	Definition
Interface	Valid slot and port number separated by a forward slash.
Neighbor IP Address	The IP address of the neighbor router.
Interface Index	The interface ID of the neighbor router.
Area ID	The area ID of the OSPF area associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
Dead Timer Due	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Up Time	Neighbor uptime; how long since the adjacency last reached the Full state.
State	The state of the neighboring routers.
Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

Example: The following shows example CLI display output for the command.

```
(alpha1) #show ip ospf neighbor 170.1.1.50

Interface.....................................0/17
Neighbor IP Address...........................170.1.1.50
Interface Index...............................17
Area Id.......................................0.0.0.2
Options.......................................0x2
```

```
Router Priority.............................1
Dead timer due in (secs).....................15
Up Time.....................................0 days 2 hrs 8 mins 46 secs
State.....................................Full/BACKUP-DR
Events.....................................4
Retransmission Queue Length..................0
```

4.8.62 show ip ospf range

This command displays information about the area ranges for the specified `areaid`. The `areaid` identifies the OSPF area whose ranges are being displayed.

Format **`show ip ospf range areaid`**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Area ID	The area id of the requested OSPF area.
IP Address	An IP address which represents this area range.
Subnet Mask	A valid subnet mask for this area range.
Lsdb Type	The type of link advertisement associated with this area range.
Advertisement	The status of the advertisement. Advertisement has two possible settings: enabled or disabled.

4.8.63 show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

Format **`show ip ospf statistics`**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Delta T	How long ago the SPF ran. The time is in the format hh:mm:ss, giving the hours, minutes, and seconds since the SPF run.
SPF Duration	How long the SPF took in milliseconds.
Reason	The reason the SPF was scheduled. Reason codes are as follows: • R - a router LSA has changed • N - a network LSA has changed • SN - a type 3 network summary LSA has changed • SA - a type 4 ASBR summary LSA has changed • X - a type 5 or type 7 external LSA has changed

4.8.64 show ip ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format `show ip ospf stub table`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Area ID	A 32-bit identifier for the created stub area.
Type of Service	The type of service associated with the stub metric. FASTPATH only supports Normal TOS.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

4.8.65 show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The `areaid` parameter identifies the area and the `neighbor` parameter identifies the neighbor's Router ID.

Format `show ip ospf virtual-link areaid neighbor`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Area ID	The area id of the requested OSPF area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Interface Transmit Delay	The configured transmit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	The configured authentication type of the OSPF virtual interface.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

4.8.66 show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

Format `show ip ospf virtual-link brief`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Area ID	The area id of the requested OSPF area.
Neighbor	The neighbor interface of the OSPF virtual interface.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Transmit Delay	The configured transmit delay for the OSPF virtual interface.

4.9 Routing Information Protocol Commands

This section describes the commands you use to view and configure Routing Information Protocol (RIP), which is a distance-vector routing protocol that you use to route traffic within a small network.

4.9.1 router rip

Use this command to enter Router RIP mode.

Format `router rip`
Mode Global Config

4.9.2 enable (RIP)

This command resets the default administrative mode of RIP in the router (active).

Default enabled
Format `enable`
Mode Router RIP Config

4.9.2.1 no enable (RIP)

This command sets the administrative mode of RIP in the router to inactive.

Format `no enable`
Mode Router RIP Config

4.9.3 ip rip

This command enables RIP on a router interface or range of interfaces.

Default disabled
Format `ip rip`
Mode Interface Config

4.9.3.1 no ip rip

This command disables RIP on a router interface.

Format `no ip rip`

Mode Interface Config

4.9.4 auto-summary

This command enables the RIP auto-summarization mode.

Default disabled

Format `auto-summary`

Mode Router RIP Config

4.9.4.1 no auto-summary

This command disables the RIP auto-summarization mode.

Format `no auto-summary`

Mode Router RIP Config

4.9.5 default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format `default-information originate`

Mode Router RIP Config

4.9.5.1 no default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format `no default-information originate`

Mode Router RIP Config

4.9.6 default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

Format `default-metric <0-15>`

Mode Router RIP Config

4.9.6.1 no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format `no default-metric`

Mode Router RIP Config

4.9.7 distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. A route with a preference of 255 cannot be used to forward traffic.

Default 15

Format **distance rip <***1-255***>**

Mode Router RIP Config

4.9.7.1 no distance rip

This command sets the default route preference value of RIP in the router.

Format **no distance rip**

Mode Router RIP Config

4.9.8 distribute-list out (RIP)

This command is used to specify the access list to filter routes received from the source protocol.

Default 0

Format **distribute-list** *<1-199>* **out** *{ospf | bgp | static | connected}*

Mode Router RIP Config

4.9.8.1 no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format **no distribute-list** *<1-199>* **out** *{ospf | bgp | static | connected}*

Mode Router RIP Config

4.9.9 ip rip authentication

This command sets the RIP Version 2 Authentication Type and Key for the specified interface or range of interfaces. The value of `type` is either *none*, *simple*, or *encrypt*. The value for authentication key [*key*] must be 16 bytes or less. The [*key*] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the value of `type` is *encrypt*, a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

Default none

Format **ip rip authentication** *{none | {simple key} | {encrypt key keyid}}*

Mode Interface Config

4.9.9.1 no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

Format **no ip rip authentication**

Mode Interface Config

4.9.10 ip rip receive version

This command configures an interface or range of interfaces to allow RIP control packets of the specified version(s) to be received.

The value for `mode` is one of: *rip1* to receive only RIP version 1 formatted packets, *rip2* for RIP version 2, *both* to receive packets from either format, or *none* to not allow any RIP control packets to be received.

Default both

Format **ip rip receive version** *{rip1 | rip2 | both | none}*

Mode Interface Config

4.9.10.1 no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format **no ip rip receive version**

Mode Interface Config

4.9.11 ip rip send version

This command configures an interface or range of interfaces to allow RIP control packets of the specified version to be sent. The value for `mode` is one of: *rip1* to broadcast RIP version 1 formatted packets, *rip1c* (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, *rip2* for sending RIP version 2 using multicast, or *none* to not allow any RIP control packets to be sent.

Default ripi2

Format **ip rip send version** *{rip1 | rip1c | rip2 | none}*

Mode Interface Config

4.9.11.1 no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

Format **no ip rip send version**

Mode Interface Config

4.9.12 hostroutesaccept

This command enables the RIP hostroutesaccept mode.

Default enabled

Format **hostroutesaccept**

Mode Router RIP Config

4.9.12.1 no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format **no hostroutesaccept**

Mode Router RIP Config

4.9.13 split-horizon

This command sets the RIP split horizon mode. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None - no special processing for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

Default simple

Format **split-horizon** *{none | simple | poison}*

Mode Router RIP Config

4.9.13.1 no split-horizon

This command sets the default RIP split horizon mode.

Format **no split-horizon**

Mode Router RIP Config

4.9.14 redistribute (RIP)

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match *match-type* the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

Default
- metric—not-configured
- match—internal

Format for OSPF as source protocol **redistribute ospf** *[metric <0-15>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]*

Format for other source protocol **redistribute** *{bgp | static | connected} [metric <0-15>]*

Mode Router RIP Config

4.9.14.1 no redistribute

This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Format **no redistribute** *{ospf | bgp | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]*

Mode Router RIP Config

4.9.15 show ip rip

This command displays information relevant to the RIP router.

Format **show ip rip**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
RIP Admin Mode	Enable or disable.
Split Horizon Mode	None, simple or poison reverse.
Auto Summary Mode	Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries The default is enable.
Host Routes Accept Mode	Enable or disable. If enabled the router accepts host routes. The default is enable.
Global Route Changes	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global queries	The number of responses sent to RIP queries from other systems.
Default Metric	The default metric of redistributed routes if one has already been set, or blank if not configured earlier. The valid values are 1 to 15.
Default Route Advertise	The default route.

4.9.16 show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e., ip rip).

Format `show ip rip interface brief`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
IP Address	The IP source address used by the specified RIP interface.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both
RIP Mode	The administrative mode of router RIP operation (enabled or disabled).
Link State	The mode of the interface (up or down).

4.9.17 show ip rip interface

This command displays information related to a particular RIP interface.

Format `show ip rip interface` *slot/port*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash. This is a configured value.

Term	Definition
IP Address	The IP source address used by the specified RIP interface. This is a configured value.
Send Version	The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.
Receive Version	The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.
Both RIP Admin Mode	RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.
Link State	Indicates whether the RIP interface is up or down. This is a configured value.
Authentication Type	The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.
Default Metric	A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value.

The following information will be invalid if the link state is down.

Term	Definition
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes contained in valid RIP packets that were ignored for any reason.
Updates Sent	The number of triggered RIP updates actually sent on this interface.

4.10 ICMP Throttling Commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

4.10.1 ip unreachables

Use this command to enable the generation of ICMP Destination Unreachable messages on an interface or range of interfaces. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default enable

Format `ip unreachables`

Mode Interface Config

4.10.1.1 no ip unreachables

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format `no ip unreachables`

Mode Interface Config

4.10.2 ip redirects

Use this command to enable the generation of ICMP Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled.

Default enable

Format `ip redirects`

Mode
- Global Config
- Interface Config

4.10.2.1 no ip redirects

Use this command to prevent the generation of ICMP Redirect messages by the router.

Format `no ip redirects`

Mode
- Global Config
- Interface Config

4.10.3 ip icmp echo-reply

Use this command to enable the generation of ICMP Echo Reply messages by the router. By default, the generation of ICMP Echo Reply messages is enabled.

Default enable

Format `ip icmp echo-reply`

Mode Global Config

4.10.3.1 no ip icmp echo-reply

Use this command to prevent the generation of ICMP Echo Reply messages by the router.

Format `no ip icmp echo-reply`

Mode Global Config

4.10.4 ip icmp error-interval

Use this command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec).

The *burst-size* is the number of ICMP error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages.

To disable ICMP rate limiting, set *burst-interval* to zero (0).

Default
- *burst-interval* of 1000 msec.
- *burst-size* of 100 messages

Format `ip icmp error-interval` *burst-interval [burst-size]*

Mode Global Config

4.10.4.1 no ip icmp error-interval

Use the **no** form of the command to return *burst-interval* and *burst-size* to their default values

Format	`no ip icmp error-interval`
Mode	Global Config

Chapter 5

IP Multicast Commands

5. IP Multicast Commands

This chapter describes the IP Multicast commands available in the FASTPATH CLI.

The IPv4 Routing and Multicast options are not available on all board variants, please contact your local Kontron representative for additional information.

The IP Multicast Commands chapter contains the following sections:

- 5.1 “Multicast Commands” on page 5 - 2
- 5.2 “DVMRP Commands” on page 5 - 6
- 5.3 “PIM-DM Commands” on page 5 - 10
- 5.4 “PIM-SM Commands” on page 5 - 12
- 5.5 “Internet Group Message Protocol Commands” on page 5 - 19
- 5.6 “IGMP Proxy Commands” on page 5 - 25

Caution! The commands in this chapter are in one of two 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.

5.1 Multicast Commands

This section describes the commands you use to configure IP Multicast and to view IP Multicast settings and statistics.

5.1.1 ip mcast boundary

This command adds an administrative scope multicast boundary specified by `groupipaddr` and `mask` for which this multicast administrative boundary is applicable. `groupipaddr` is a group IP address and `mask` is a group IP mask. This command can be used to configure a single interface or a range of interfaces.

Format **`ip mcast boundary`** *`groupipaddr mask`*

Mode Interface Config

5.1.1.1 no ip mcast boundary

This command deletes an administrative scope multicast boundary specified by `groupipaddr` and `mask` for which this multicast administrative boundary is applicable. `groupipaddr` is a group IP address and `mask` is a group IP mask.

Format **`no ip mcast boundary`** *`groupipaddr mask`*

Mode Interface Config

5.1.2 ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active.

Default disabled

Format `ip multicast`
Mode Global Config

5.1.2.1 no ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to inactive.

Format `no ip multicast`
Mode Global Config

5.1.3 ip multicast ttl-threshold

This command is specific to IPv4. Use this command to apply the given Time-to-Live threshold value `ttl-threshold` to a routing interface or range of interfaces. The `ttl-threshold` is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. This command sets the Time-to-Live threshold value such that any data packets forwarded over the interface having TTL value above the configured value are dropped. The value for `ttl-threshold` ranges from 0 to 255.

Default 1
Format `ip multicast ttl-threshold ttlvalue`
Mode Interface Config

5.1.3.1 no ip multicast ttl-threshold

This command applies the default `ttl-threshold` to a routing interface. The `ttl-threshold` is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Format `no ip multicast ttl-threshold`
Mode Interface Config

5.1.4 show ip mcast

This command displays the system-wide multicast information.

Format `show ip mcast`
Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Admin Mode	The administrative status of multicast. Possible values are enabled or disabled.
Protocol State	The current state of the multicast protocol. Possible values are Operational or Non-Operational.
Table Max Size	The maximum number of entries allowed in the multicast table.
Protocol	The multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.
Multicast Forwarding Cache Entry Count	The number of entries in the multicast forwarding cache.

5.1.5 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Format **show ip mcast boundary** *{slot/port | all}*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
Group Ip	The group IP address.
Mask	The group IP mask.

5.1.6 show ip mcast interface

This command displays the multicast information for the specified interface.

Format **show ip mcast interface** *slot/port*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
TTL	The time-to-live value for this interface.

5.1.7 show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Format **show ip mcast mroute** *{detail | summary}*

Modes
- Privileged EXEC
- User EXEC

If you use the *detail* parameter, the command displays the following fields:

Term	*Definition*
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the *summary* parameter, the command displays the following fields:

Term	*Definition*
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which the entry was created.
Incoming Interface	The interface on which the packet for the source/group arrives.
Outgoing Interface List	The list of outgoing interfaces on which the packet is forwarded.

5.1.8 show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given `groupipaddr`.

Format **`show ip mcast mroute group`** *`groupipaddr {detail |summary}`*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this group arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

5.1.9 show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given source IP address or source IP address and group IP address pair.

Format **`show ip mcast mroute source`** *`sourceipaddr {summary | groupipaddr}`*

Modes
- Privileged EXEC
- User EXEC

If you use the *`groupipaddr`* parameter, the command displays the following column headings in the output table:

Term	*Definition*
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.

Term	*Definition*
Flags	The flags associated with this entry.

If you use the *summary* parameter, the command displays the following column headings in the output table:

Term	*Definition*
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this source arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

5.2 DVMRP Commands

This section provides a detailed explanation of the Distance Vector Multicast Routing Protocol (DVMRP) commands.

5.2.1 ip dvmrp

This command sets administrative mode of DVMRP in the router to active.

Default disabled

Format **`ip dvmrp`**

Mode Global Config

5.2.1.1 no ip dvmrp

This command sets administrative mode of DVMRP in the router to inactive.

Format **`no ip dvmrp`**

Mode Global Config

5.2.2 ip dvmrp metric

This command configures the metric for an interface or range of interfaces. This value is used in the DVMRP messages as the cost to reach this network. This field has a range of 1 to 31.

Default 1

Format **`ip dvmrp metric`** metric

Mode Interface Config

5.2.2.1 no ip dvmrp metric

This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

Format **`no ip dvmrp metric`**

Mode Interface Config

5.2.3 ip dvmrp trapflags

This command enables the DVMRP trap mode.

Default disabled
Format `ip dvmrp trapflags`
Mode Global Config

5.2.3.1 no ip dvmrp trapflags

This command disables the DVMRP trap mode.

Format `no ip dvmrp trapflags`
Mode Global Config

5.2.4 ip dvmrp

This command sets the administrative mode of DVMRP on an interface or range of interfaces to active.

Default disabled
Format `ip dvmrp`
Mode Interface Config

5.2.4.1 no ip dvmrp

This command sets the administrative mode of DVMRP on an interface to inactive.

Format `no ip dvmrp`
Mode Interface Config

5.2.5 show ip dvmrp

This command displays the system-wide information for DVMRP.

Format `show ip dvmrp`
Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Admin Mode	Indicates whether DVMRP is enabled or disabled.
Version String	The version of DVMRP being used.
Number of Routes	The number of routes in the DVMRP routing table.
Reachable Routes	The number of entries in the routing table with non-infinite metrics.

The following fields are displayed for each interface.

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.

Term	Definition
Interface Mode	The mode of this interface. Possible values are Enabled and Disabled.
State	The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.

5.2.6 show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

Format `show ip dvmrp interface` *slot/port*

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface Mode	Indicates whether DVMRP is enabled or disabled on the specified interface.
Metric	The metric of this interface. This is a configured value.
Local Address	The IP address of the interface.

The following field is displayed only when DVMRP is operational on the interface.

Term	Definition
Generation ID	The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

The following fields are displayed only if DVMRP is enabled on this interface.

Term	Definition
Received Bad Packets	The number of invalid packets received.
Received Bad Routes	The number of invalid routes received.
Sent Routes	The number of routes that have been sent on this interface.

5.2.7 show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

Format `show ip dvmrp neighbor`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IfIndex	The value of the interface used to reach the neighbor.
Nbr IP Addr	The IP address of the DVMRP neighbor for which this entry contains information.
State	The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.
Up Time	The time since this neighboring router was learned.

Term	*Definition*
Expiry Time	The time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.
Generation ID	The Generation ID value for the neighbor.
Major Version	The major version of DVMRP protocol of neighbor.
Minor Version	The minor version of DVMRP protocol of neighbor.
Capabilities	The capabilities of neighbor.
Received Routes	The number of routes received from the neighbor.
Rcvd Bad Pkts	The number of invalid packets received from this neighbor.
Rcvd Bad Routes	The number of correct packets received with invalid routes.

5.2.8 show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Format `show ip dvmrp nexthop`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Source IP	The sources for which this entry specifies a next hop on an outgoing interface.
Source Mask	The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.
Next Hop Interface	The interface in slot/port format for the outgoing interface for this next hop.
Type	The network is a LEAF or a BRANCH.

5.2.9 show ip dvmrp prune

This command displays the table listing the router's upstream prune information.

Format `show ip dvmrp prune`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Group IP	The multicast Address that is pruned.
Source IP	The IP address of the source that has pruned.
Source Mask	The network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.
Expiry Time (secs)	The expiry time in seconds. This is the time remaining for this prune to age out.

5.2.10 show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Format `show ip dvmrp route`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Source Address	The multicast address of the source group.
Source Mask	The IP Mask for the source group.
Upstream Neighbor	The IP address of the neighbor which is the source for the packets for a specified multicast address.
Interface	The interface used to receive the packets sent by the sources.
Metric	The distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.
Expiry Time (secs)	The expiry time in seconds, which is the time left for this route to age out.
Up Time (secs)	The time when a specified route was learnt, in seconds.

5.3 PIM-DM Commands

This section describes the commands you use to configure Protocol Independent Multicast -Dense Mode (PIM-DM). PIM-DM is a multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol.

5.3.1 ip pimdm (Global Config)

This command enables the administrative mode of PIM-DM in the router.

Default disabled

Format `ip pimdm`

Mode Global Config

5.3.1.1 no ip pimdm (Global Config)

This command disables the administrative mode of PIM-DM in the router.

Format `no ip pimdm`

Mode Global Config

5.3.2 ip pimdm (Interface Config)

This command sets administrative mode of PIM-DM on an interface or range of interfaces to enabled.

Default disabled

Format `ip pimdm`

Mode Interface Config

5.3.2.1 no ip pimdm mode (Interface Config)

This command sets administrative mode of PIM-DM on an interface to disabled.

Format `no ip pimdm`

Mode Interface Config

5.3.3 ip pimdm hello-interval

This command configures the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 1 to 3600 seconds.

Default 30

Format **`ip pimdm hello-interval`** *seconds*

Mode Interface Config

5.3.3.1 no ip pimdm hello-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format **`no ip pimdm hello-interval`**

Mode Interface Config

5.3.4 show ip pimdm

This command displays the system-wide information for PIM-DM.

Format **`show ip pimdm`**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
PIM-DM Admin Mode	Indicates whether PIM-DM is enabled or disabled.
Interface	Valid slot and port number separated by a forward slash.
Interface Mode	Indicates whether PIM-DM is enabled or disabled on this interface.
State	The current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

5.3.5 show ip pimdm interface

This command displays the interface information for PIM-DM on the specified interface.

Format **`show ip pimdm interface`** *<slot/port>*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface Mode	Indicates whether PIM-DM is enabled or disabled on the specified interface.
PIM-DM Interface Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

5.3.6 show ip pimdm interface stats

This command displays the statistical information for PIM-DM on the specified interface.

Format **show ip pimdm interface stats** *{slot/port | all}*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
IP Address	The IP address that represents the PIM-DM interface.
Nbr Count	The neighbor count for the PIM-DM interface.
Hello Interval	The time interval between two hello messages sent from the router on the given interface.
Designated Router	The IP address of the Designated Router for this interface.

5.3.7 show ip pimdm neighbor

This command displays the neighbor information for PIM-DM on the specified interface.

Format **show ip pimdm neighbor** *{slot/port | all}*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Neighbor Address	The IP address of the neighbor on an interface.
Interface	Valid slot and port number separated by a forward slash.
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.

5.4 PIM-SM Commands

This section describes the commands you use to configure Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-SM is a multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol.

5.4.1 ip pimsm

This command is used to administratively enable PIM-SM multicast routing mode on a particular router interface.

Default disabled

Format **ip pimsm**

Mode Interface Config

5.4.1.1 no ip pimsm

This command is used to administratively disable PIM-SM multicast routing mode on a particular router interface.

Format `no ip pimsm`
Mode Interface Config

5.4.2 ip pimsm bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface or range of interfaces.

Default disabled
Format `ip pimsm bsr-border`
Mode Interface Config

5.4.2.1 no ip pimsm bsr-border

Use this command to disable the interface from being the BSR border.

Format `no ip pimsm bsr-border`
Mode Interface Config

5.4.3 ip pimsm bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

Default None
Format `ip pimsm bsr-candidate interface` *slot/port [hash-mask-length] [priority]*
Mode Global Config

Parameters	*Description*
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
priority	Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

5.4.3.1 no ip pimsm bsr-candidate

This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

Format `no ip pimsm bsr-candidate interface` *slot/port [hash-mask-length] [priority]*
Mode Global Config

5.4.4 ip pimsm dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR). This command can be used on a single interface or a range of interfaces.

Default 1
Format **`ip pimsm dr-priority <0-2147483647>`**
Mode Interface Config

5.4.4.1 no ip pimsm dr-priority

Use this command to disable the interface from being the BSR border.

Format **`no ip pimsm dr-priority`**
Mode Interface Config

5.4.5 ip pimsm hello-interval

This command is used to configure the PIM-SM hello interval for the specified interface or range of interfaces. The hello interval is specified in seconds.

Default 30
Format **`ip pimsm hello-interval`** *`<0-18000>`*
Mode Interface Config

5.4.5.1 no ip pimsm hello-interval

This command is used to set the hello interval to the default value.

Format **`no ip pimsm hello-interval`**
Mode Interface Config

5.4.6 ip pimsm join-prune-interval

This command is used to configure the join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

Default 60
Format **`ip pimsm join-prune-interval`** *`<0-18000>`*
Mode Interface Config

5.4.6.1 no ip pimsm join-prune-interval

Use this command to set the join/prune interval to the default value.

Format **`no ip pimsm join-prune-interval`**
Mode Interface Config

5.4.7 ip pimsm register-threshold

This command configures the Register Threshold rate for the Rendezvous Point router to switch to a source-specific shortest path. The valid values are from (0 to 2000 kilobits/sec).

Default 0

Format **ip pimsm register-threshold** *<0-2000>*

Mode Global Config

5.4.7.1 no ip pimsm register-threshold

This command resets the register threshold rate for the Rendezvous Pointer router to the default value.

Format **no ip pimsm register-threshold**

Mode Global Config

5.4.8 ip pimsm rp-address

This command is used to statically configure the RP address for one or more multicast groups. The parameter *rp-address* is the IP address of the RP. The parameter *groupaddress* is the group address supported by the RP. The parameter *groupmask* is the group mask for the group address. The optional keyword *override* indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Default 0

Format **ip pimsm rp-address** *rp-address group-address group-mask* **[override]**

Mode Global Config

5.4.8.1 no ip pimsm rp-address

This command is used to statically remove the RP address for one or more multicast groups.

Format **no ip pimsm rp-address** *rp-address group-address group-mask*

Mode Global Config

5.4.9 ip pimsm rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Default None

Format **ip pimsm rp-candidate interface** *slot/port group-address group-mask*

Mode Global Config

5.4.9.1 no ip pimsm rp-candidate

This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format **no ip pimsm rp-candidate interface** *slot/port group-address group-mask*

Mode Global Config

5.4.10 ip pimsm spt-threshold

This command is used to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The rate is specified in Kilobits per second. The possible values are 1 to 2000.

Default 0

Format **`ip pimsm spt-threshold`** *<1-2000>*

Mode Global Config

5.4.10.1 no ip pimsm spt-threshold

This command is used to set the Data Threshold rate for the RP router to the default value.

Format **`no ip pimsm spt-threshold`**

Mode Global Config

5.4.11 ip pimsm ssm

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

Default disabled

Format **`ip pimsm ssm`** *{default | group-address group-mask}*

Mode Global Config

Parameter	*Description*
default-range	Defines the SSM range access list to 232/8.

5.4.11.1 no ip pimsm ssm

This command is used to disable the Source Specific Multicast (SSM) range.

Format **`no ip pimsm ssm`**

Mode Global Config

5.4.12 ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Default disabled

Format **`ip pim-trapflags`**

Mode Global Config

5.4.12.1 no ip pim-trapflags

This command sets the PIM trap mode to the default.

Format **`no ip pim-trapflags`**

Mode Global Config

5.4.13 show ip pimsm

This command displays the system-wide information for PIM-SM.

Format `show ip pimsm`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
PIM-SM Admin Mode	Indicates whether PIM-SM is enabled or disabled.
Data Threshold Rate (Kbps)	The data threshold rate for the PIM-SM router.
Register Threshold Rate (Kbps)	The threshold rate for the RP router to switch to the shortest path.
Interface	Valid slot and port number separated by a forward slash.
Interface Mode	Indicates whether PIM-SM is enabled or disabled on the interface.
Protocol State	The current state of the PIM-SM protocol on the interface. Possible values are Operational or Non-Operational.

5.4.14 show ip pimsm bsr

This command displays the bootstrap router (BSR) information. The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Format `show ip pimsm bsr`

Mode
- Privileged EXEC
- User EXEC

Term	*Definition*
BSR Address	IP address of the BSR.
Uptime	Length of time that this router has been up (in hours, minutes, and seconds).
BSR Priority	Priority as configured in the `ip pimsm bsr-candidate` command.
Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the `ip pimsm bsr-candidate` command.
Next Bootstrap Message In	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP advertisement in	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

5.4.15 show ip pimsm interface

This command displays interface configuration parameters for PIM-SM on the specified interface. If no interface is specified, all interfaces are displayed.

Format `show ip pimsm interface` [*slot/port*]

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Slot Port	Valid slot and port number separated by a forward slash.
IP Address	The IP address of the specified interface.
Subnet Mask	The Subnet Mask for the IP address of the PIM interface.
Hello Interval (secs)	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.
Join Prune Interval (secs)	The join/prune interval for the PIM-SM router. The interval is in seconds.
Neighbor Count	The neighbor count for the PIM-SM interface.
Designated Router	The IP address of the Designated Router for this interface.
DR Priority	The priority of the Designated Router.
BSR Border	The bootstrap router border interface. Possible values are *enabled* or *disabled*.

Example: The following shows example CLI display output for the command.

```
(Router) #show ip pimsm interface 0/3

Slot/Port..................................... 0/3
IP Address.................................... 41.1.1.2
Subnet Mask................................... 255.255.255.0
Hello Interval (secs)......................... 30
Join Prune Interval (secs).................... 60
Neighbor Count ............................... 0
Designated Router............................. 41.1.1.2
DR Priority................................... 1
BSR Border.................................... Disabled
```

5.4.16 show ip pimsm neighbor

This command displays the neighbor information for PIM-SM on the specified interface.

Format **show ip pimsm neighbor** *{slot/port | all}*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
IP Address	The IP address of the neighbor on an interface.
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.

5.4.17 show ip pimsm rphash

This command displays which rendezvous point (RP) is being used for a specified group.

Format **show ip pimsm rphash <***group-address***>**

Modes
- Privileged EXEC
- User EXEC

Term	Definition
RP	The IP address of the RP for the group specified.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.

5.4.18 show ip pimsm rp mapping

Use this command to display all group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). If no RP is specified, all active RPs are displayed.

Format `show ip pimsm rp mapping [rp address]`

Modes
- Privileged EXEC
- User EXEC

5.5 Internet Group Message Protocol Commands

This section describes the commands you use to view and configure Internet Group Message Protocol (IGMP) settings.

5.5.1 ip igmp

This command sets the administrative mode of IGMP in the system to active on an interface or range of interfaces.

Default disabled

Format `ip igmp`

Modes
- Global Config
- Interface Config

5.5.1.1 no ip igmp

This command sets the administrative mode of IGMP in the system to inactive.

Format `no ip igmp`

Modes
- Global Config
- Interface Config

5.5.2 ip igmp version

This command configures the version of IGMP for an interface. The value for *version* is either 1, 2 or 3.

Default 3

Format `ip igmp version version`

Modes Interface Config

5.5.2.1 no ip igmp version

This command resets the version of IGMP to the default value.

Format `no ip igmp version`

Modes Interface Config

5.5.3 ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent by the interface or range of interfacesinterface or range of interfacesinterface or range of interfaces before the router assumes that there are no local members on the interface. The range for *count* is 1 to 20.

Format **ip igmp last-member-query-count** *count*

Modes Interface Config

5.5.3.1 no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

Format **no ip igmp last-member-query-count**

Modes Interface Config

5.5.4 ip igmp last-member-query-interval

This command configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages. The range for `seconds` is 0 to 255 tenths of a second.

Default 10 tenths of a second (1 second)

Format **ip igmp last-member-query-interval seconds**

Modes Interface Config

5.5.4.1 no ip igmp last-member-query-interval

This command resets the Maximum Response Time to the default value.

Format **no ip igmp last-member-query-interval**

Modes Interface Config

5.5.5 ip igmp query-interval

This command configures the query interval for the specified interface or range of interfaces. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for *queryinterval* is 1 to 3600 seconds.

Default 125 seconds

Format **ip igmp query-interval seconds**

Modes Interface Config

5.5.5.1 no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format **no ip igmp query-interval**

Modes Interface Config

5.5.6 ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface.The time interval is specified in tenths of a second. The range for `<maxresptime>` is 0 to 255 tenths of a second.

Default 100

Format **`ip igmp query-max-response-time seconds`**

Mode Interface Config

5.5.6.1 no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format **`no ip igmp query-max-response-time`**

Mode Interface Config

5.5.7 ip igmp robustness

This command configures the robustness that allows tuning of the interface or range of interfaces. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface. The range for `robustness` is 1 to 255.

Default 2

Format **`ip igmp robustness robustness`**

Mode Interface Config

5.5.7.1 no ip igmp robustness

This command sets the robustness value to default.

Format **`no ip igmp robustness`**

Mode Interface Config

5.5.8 ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface or range of interfaces. The range for `count` is 1 to 20.

Default 2

Format **`ip igmp startup-query-count count`**

Mode Interface Config

5.5.8.1 no ip igmp startup-query-count

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format `no ip igmp startup-query-count`

Mode Interface Config

5.5.9 ip igmp startup-query-interval

This command sets the interval between General Queries sent on startup on the interface. The time interval value is in seconds. The range for `interval` is 1 to 300 seconds.

Default 31

Format `ip igmp startup-query-interval interval`

Mode Interface Config

5.5.9.1 no ip igmp startup-query-interval

This command resets the interval between General Queries sent on startup on the interface to the default value.

Format `no ip igmp startup-query-interval`

Mode Interface Config

5.5.10 show ip igmp

This command displays the system-wide IGMP information.

Format `show ip igmp`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
IGMP Admin Mode	The administrative status of IGMP. This is a configured value.
Interface	Valid slot and port number separated by a forward slash.
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Protocol State	The current state of IGMP on this interface. Possible values are Operational or Non-Operational.

5.5.11 show ip igmp groups

This command displays the registered multicast groups on the interface. If *[detail]* is specified this command displays the registered multicast groups on the interface in detail.

Format `show ip igmp groups <slot/port> [detail]`

Mode Privileged EXEC

If you do not use the **detail** keyword, the following fields appear:

Term	*Definition*
IP Address	The IP address of the interface participating in the multicast group.
Subnet Mask	The subnet mask of the interface participating in the multicast group.
Interface Mode	This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled:

Term	*Definition*
Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	The list of multicast groups that are registered on this interface.

If you use the **detail** keyword, the following fields appear:

Term	*Definition*
Multicast IP Address	The IP address of the registered multicast group on this interface.
Last Reporter	The IP address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	The time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	The amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.
Version2 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 2 host present.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

5.5.12 show ip igmp interface

This command displays the IGMP information for the interface.

Format **show ip igmp interface** *slot/port*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	Valid slot and port number separated by a forward slash.
IGMP Admin Mode	The administrative status of IGMP.
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface.
IGMP Version	The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.
Query Interval	The frequency at which IGMP Host-Query packets are transmitted on this interface.

Term	Definition
Query Max Response Time	The maximum query response time advertised in IGMPv2 queries on this interface.
Robustness	The tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface.
Startup Query Interval	The interval between General Queries sent by a Querier on startup.
Startup Query Count	The number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	The number of Group-Specific Queries sent before the router assumes that there are no local members.

5.5.13 show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

Format **`show ip igmp interface membership`** *<multiipaddr> [detail]*

Mode Privileged EXEC

Term	Definition
Interface	Valid unit, slot and port number separated by forward slashes.
Interface IP	The IP address of the interface participating in the multicast group.
State	The interface that has IGMP in Querier mode or Non-Querier mode.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

If you use the **`detail`** keyword, the following fields appear:

Term	Definition
Interface	Valid unit, slot and port number separated by forward slashes.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Source Hosts	The list of unicast source IP addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP address. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Expiry Time	The amount of time remaining to remove this entry before it is aged out. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

5.5.14 show ip igmp interface stats

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

Format `show ip igmp interface stats` *<slot/port>*

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Querier Status	The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.
Querier IP Address	The IP address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	The time since the interface Querier was last changed.
Querier Expiry Time	The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.
Wrong Version Queries	The number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Groups	The current number of membership entries for this interface.

5.6 IGMP Proxy Commands

The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

5.6.1 ip igmp-proxy

This command enables the IGMP Proxy on an interface or range of interfaces. To enable the IGMP Proxy on an interface, you must enable multicast forwarding. Also, make sure that there are no multicast routing protocols enabled on the router.

Format `ip igmp-proxy`

Mode Interface Config

5.6.1.1 no ip igmp-proxy

This command disables the IGMP Proxy on the router.

Format `no ip igmp-proxy`

Mode Interface Config

5.6.2 ip igmp-proxy unsolicit-rprt-interval

This command sets the unsolicited report interval for the IGMP Proxy interface or range of interfaces. This command is valid only when you enable IGMP Proxy on the interface or range of interfaces. The value of *interval* can be 1-260 seconds.

Default 1

Format `ip igmp-proxy unsolicit-rprt-interval` *interval*

Mode Interface Config

5.6.2.1 no ip igmp-proxy unsolicit-rprt-interval

This command resets the unsolicited report interval of the IGMP Proxy router to the default value.

Format `no ip igmp-proxy unsolicit-rprt-interval`

Mode Interface Config

5.6.3 ip igmp-proxy reset-status

This command resets the host interface status parameters of the IGMP Proxy interface or range of interfaces. This command is valid only when you enable IGMP Proxy on the interface.

Format `ip igmp-proxy reset-status`

Mode Interface Config

5.6.4 show ip igmp-proxy

This command displays a summary of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format `show ip igmp-proxy`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface index	The interface number of the IGMP Proxy.
Admin Mode	States whether the IGMP Proxy is enabled or not. This is a configured value.
Operational Mode	States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.
Version	The present IGMP host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the IGMP Proxy interface.
Unsolicited Report Interval	The time interval at which the IGMP Proxy interface sends unsolicited group membership report.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Older Version 2 Querier Timeout	The interval used to timeout the older version 2 queriers.
Proxy Start Frequency	The number of times the IGMP Proxy has been stopped and started.

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show ip igmp-proxy
```

```
Interface Index..................................... 0/1
Admin Mode.......................................... Enable
Operational Mode.................................... Enable
Version............................................. 3
Num of Multicast Groups............................. 0
Unsolicited Report Interval......................... 1
Querier IP Address on Proxy Interface............... 5.5.5.50
Older Version 1 Querier Timeout..................... 0
Older Version 2 Querier Timeout..................... 00::00:00
Proxy Start Frequency............................... 1
```

5.6.5 show ip igmp-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format **`show ip igmp-proxy interface`**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface Index	The slot/port of the IGMP proxy.

The column headings of the table associated with the interface are as follows:

Term	*Definition*
Ver	The IGMP version.
Query Rcvd	Number of IGMP queries received.
Report Rcvd	Number of IGMP reports received.
Report Sent	Number of IGMP reports sent.
Leaves Rcvd	Number of IGMP leaves received. Valid for version 2 only.
Leaves Sent	Number of IGMP leaves sent on the Proxy interface. Valid for version 2 only.

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show ip igmp-proxy interface

Interface Index.............................. 0/1

Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-----------------------------------------------------------------
1      0            0            0         -----       -----
2      0            0            0          0           0
3      0            0            0         -----       -----
```

5.6.6 show ip igmp-proxy groups

This command displays information about the subscribed multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format **`show ip igmp-proxy groups`**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group on the network attached to the IGMP Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. • IDLE_MEMBER - interface has responded to the latest group membership query for this group. • DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are **Include** or **Exclude**.
Sources	The number of sources attached to the multicast group.

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show ip igmp-proxy groups

Interface Index.............................. 0/1

Group Address    Last Reporter    Up Time   Member State  Filter Mode  Sources
-------------    -------------- ---------- ------------- ------------- -------
225.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include       3

226.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include       3

227.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Exclude       0

228.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include       3
```

5.6.7 show ip igmp-proxy groups detail

This command displays complete information about multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format `show ip igmp-proxy groups detail`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group, on the network attached to the IGMP-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.

Term	*Definition*
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. • IDLE_MEMBER - interface has responded to the latest group membership query for this group. • DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are **Include** or **Exclude**.
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	Time left before a source is deleted.

Example: The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show ip igmp-proxy groups

Interface Index.............................. 0/1

Group Address    Last Reporter    Up Time   Member State Filter Mode  Sources
-------------    -------------- ----------- ------------ ------------ ---------
225.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include          3

Group Source List             Expiry Time
-----------------           -----------------
5.1.2.3                       00:02:21
6.1.2.3                       00:02:21
7.1.2.3                       00:02:21

226.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include          3

Group Source List             Expiry Time
-----------------           ---------------
2.1.2.3                       00:02:21
6.1.2.3                       00:01:44
8.1.2.3                       00:01:44

227.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Exclude         0



228.4.4.4        5.5.5.48         00:03:21  DELAY_MEMBER     Include          3

Group Source List             Expiry Time
-----------------           ---------------
9.1.2.3                       00:03:21
6.1.2.3                       00:03:21
7.1.2.3                       00:03:21
```

Chapter 4

Utility Commands

6. Utility Commands

This chapter describes the utility commands available in the FASTPATH CLI.

The Utility Commands chapter includes the following sections:

- 6.1 “Dual Image Commands“ on page 6 - 2
- 6.2 “System Information and Statistics Commands“ on page 6 - 3
- 6.3 “Logging Commands“ on page 6 - 15
- 6.4 “System Utility and Clear Commands“ on page 6 - 19
- 6.5 “Commands to configure startup services“ on page 6 - 32
- 6.6 “Commands supporting SFP/SFP+ (AM4910 only)“ on page 6 - 33
- 6.7 “Simple Network Time Protocol Commands“ on page 6 - 34
- 6.8 “DHCP Server Commands“ on page 6 - 39
- 6.9 “DNS Client Commands“ on page 6 - 49
- 6.10 “Serviceability Packet Tracing Commands“ on page 6 - 53
- 6.11 “Cable Test Command“ on page 6 - 59
- 6.12 “sFlow Commands“ on page 6 - 60
- 6.13 “AutoInstall Commands“ on page 6 - 62

Note: 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.

6.1 Dual Image Commands

FASTPATH software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

6.1.1 delete

This command deletes the supplied image file from the permanent storage. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, an error message displays.

Format	**delete** *{image1 | image2}*
Mode	Privileged EXEC

6.1.2 delete nvram:file <file>

This command deletes a specified file <file>. The specified filename can be a relative name related to the configuration directory or an absolute filename.

Format	**delete** *nvram:file <file>*
Mode	Privileged EXEC

6.1.3 boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots.

Format `boot system` *<image-file-name>*

Mode Privileged EXEC

6.1.4 show bootvar

This command displays the version information and the activation status for the current active and backup images. The command also displays any text description associated with an image. This command displays the switch activation status.

Format `show bootvar`

Mode Privileged EXEC

6.2 System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

6.2.1 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

Term	*Definition*
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.

6.2.2 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

Term	*Definition*
File	The file in which the event originated.
Line	The line number of the event.

Term	Definition
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.

6.2.3 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 the command 6.2.4 “show version“ on page 6 - 4.

Format **`show hardware`**

Mode Privileged EXEC

6.2.4 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

Term	Definition
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.

6.2.5 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>*, are as follows:

Parameters	*Definition*
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” are as follows:

Term	*Definition*
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.

6.2.6 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

When you specify a value for *<slot/port>*, the command displays the following information.

Term	*Definition*
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.

Term	*Definition*
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.

Term	*Definition*
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.

Term	*Definition*
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.

Term	*Definition*
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.

Term	Definition
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.

6.2.7 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.

Term	Definition
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.

Term	Definition
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:

Term	Definition
VLAN ID	The VLAN on which the MAC address was learned.

The following information displays if you enter the *count* parameter:

Term	Definition
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.

6.2.8 show process cpu

This command provides the percentage utilization of the CPU by different tasks.

Note: It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

Format `show process cpu`

Mode Privileged EXEC

The following shows example CLI display output for the command.

```
(Broadcom FASTPATH Routing) #show process cpu
Mem: 52416K used, 74048K free, 0K shrd, 0K buff, 24976K cached
Load average: 0.16, 0.18, 0.12    (State: S = sleeping R = running, W = waiting)
```

```
PID USER     STATUS   RSS  PPID %CPU %MEM COMMAND
409 root     R        704   408 15.2  0.5 exe
298 root     S        28M     1  5.0 22.8 switchdrvr
315 root     S        28M     1  2.5 22.8 switchdrvr
297 root     S        28M     1  0.8 22.8 switchdrvr
345 root     S        28M     1  0.8 22.8 switchdrvr
351 root     S        28M     1  0.0 22.8 switchdrvr
380 root     S        28M     1  0.0 22.8 switchdrvr
301 root     S        28M     1  0.0 22.8 switchdrvr
357 root     S        28M     1  0.0 22.8 switchdrvr
361 root     S        28M     1  0.0 22.8 switchdrvr
369 root     S        28M     1  0.0 22.8 switchdrvr
389 root     S        28M     1  0.0 22.8 switchdrvr
295 root     S        28M     1  0.0 22.8 switchdrvr
348 root     S        28M     1  0.0 22.8 switchdrvr
310 root     S        28M     1  0.0 22.8 switchdrvr
367 root     R        28M     1  0.0 22.8 switchdrvr
363 root     S        28M     1  0.0 22.8 switchdrvr
311 root     S        28M     1  0.0 22.8 switchdrvr
332 root     S        28M     1  0.0 22.8 switchdrvr
360 root     S        28M     1  0.0 22.8 switchdrvr
```

6.2.9 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.

Note: If you use a text-based configuration file, the **show running-config** command will only display configured physical interfaces, i.e. if any interface only contains the default configuration, that interface will be skipped from the **show running-config** command output. This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its 'exit' command, are both omitted from the **show running-config** command output (and hence from the startup-config file when the system configuration is saved.)

This command captures the current settings of OSPFv2 and OSPFv3 trapflag status:

- If all the flags are enabled, then the command displays **trapflags all**.
- If all the flags in a particular group are enabled, then the command displays **trapflags** *<group name>* **all**.
- If some, but not all, of the flags in that group are enabled, the command displays **trapflags** *<groupname> <flag-name>.*

Format **show running-config** *[all | <scriptname>]*

Mode Privileged EXEC

6.2.10 show sysinfo

This command displays switch information.

Format **show sysinfo**

Mode Privileged EXEC

Term	*Definition*
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 7.9.1 “snmp-server“ on page 7 - 28.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see 7.9.1 “snmp-server“ on page 7 - 28.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see 7.9.1 “snmp-server“ on page 7 - 28.
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.

6.2.11 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 isdp neighbors
- show logging
- show event log
- show logging buffered
- show trap log
- show running config

Format **show tech-support**

Mode Privileged EXEC

6.2.12 terminal length

Use this command to set the number of lines of output to be displayed on the screen, i.e. pagination, for the **show running-config** and **show running-config all** commands. The terminal length size is either zero or a number in the range of 5 to 48. After the user-configured number of lines is displayed in one page, the system prompts the user for `--More-- or (q)uit. Press q or Q to quit, or press any key to display`

the next set of <5-48> lines. The command **terminal length 0** disables pagination and, as a result, the output of the **show running-config** command is displayed immediately.

Default	24 lines per page
Format	**terminal length <**0|*5-48*>
Mode	Privileged EXEC

6.2.12.1 no terminal length

Use this command to set the terminal length to the default value.

6.2.13 show terminal length

Use this command to display the value of the user-configured terminal length size.

Format	**show terminal length**
Mode	Privileged EXEC

6.3 Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

6.3.1 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

6.3.1.1 no logging buffered

This command disables logging to in-memory log.

Format	**no logging buffered**
Mode	Global Config

6.3.2 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

6.3.2.1 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

6.3.3 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

6.3.3.1 no logging cli-command

This command disables the CLI command Logging feature.

Format **no logging cli-command**

Mode Global Config

6.3.4 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

6.3.4.1 no logging console

This command disables logging to the console.

Format **no logging console**

Mode Global Config

6.3.5 logging host

This command enables logging to a host. You can configure up to eight hosts. The *<ipaddr|hostname>* is the IP address of the logging host. The *<addresstype>* indicates the type of address ipv4 or ipv6 or dns being passed. 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|hostname> <addresstype> [<port>][<severitylevel>]*

Mode Global Config

6.3.6 logging host remove

This command disables logging to host. See 6.3.11 “show logging hosts“ on page 6 - 18 for a list of host indexes.

Format **logging host remove** *<hostindex>*

Mode Global Config

6.3.7 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

6.3.7.1 no logging port

This command resets the local logging port to the default.

Format **no logging port**

Mode Global Config

6.3.8 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

6.3.8.1 no logging syslog

This command disables syslog logging.

Format **no logging syslog**

Mode Global Config

6.3.9 show logging

This command displays logging configuration information.

Format `show logging`

Mode Privileged EXEC

Term	*Definition*
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.

6.3.10 show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format `show logging buffered`

Mode Privileged EXEC

Term	*Definition*
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.

6.3.11 show logging hosts

This command displays all configured logging hosts.

Format `show logging hosts`

Mode Privileged EXEC

Term	*Definition*
Host Index	(Used for deleting hosts.)

Term	*Definition*
IP Address / Hostname	IP address or hostname 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	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.

6.3.12 show logging traplogs

This command displays SNMP trap events and statistics.

Format `show logging traplogs`

Mode Privileged EXEC

Term	*Definition*
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.

6.3.13 show nvram:file

This command displays the files existing in the configuration directory (without argument) or related to the argument <file>. The argument may contain a relative or absolute pathname and/or a filename with or without wild-card characters. The file are listed in alphabetical order.

This command is using the Shell command “ls -1 <file>”.

Format `show nvram:file`
`show nvram:file` *<file>*

Mode Privileged EXEC

6.4 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.

6.4.1 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. Traceroute continues to provide a synchronous response when initiated from the CLI.

Default
- count: 3 probes
- interval: 3 seconds
- size: 0 bytes
- port: 33434
- maxTtl: 30 hops
- maxFail: 5 probes
- initTtl: 1 hop
-

Format **traceroute** <*ipaddr|hostname*> [**initTtl** <*initTtl*>] [**maxTtl** <*maxTtl*>] [**maxFail** <*maxFail*>] [**interval** <*interval*>] [**count** <*count*>] [**port** <*port*>] [**size** <*size*>]

Mode Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	*Description*
ipaddr|hostname	The *ipaddr* value should be a valid IP address. The *hostname* value should be a valid hostname.
initTtl	Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use maxTtle to specify the maximum TTL. Range is 1 to 255.
maxFail	Use maxFail to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
interval	Use interval to specify the time between probes, in seconds. Range is 1 to 60 seconds.
count	Use the optional count parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional port parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

Example: The following are examples of the CLI command.

Example: traceroute Success:

```
(Broadcom FASTPATH Routing) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0
interval 1 count 3 port 33434 size 43
 Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1   708 msec     41 msec     11 msec
2 10.240.10.115   0 msec     0 msec     0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

Example: traceroute Failure:

```
(Broadcom FASTPATH Routing) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count
3
port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

6.4.2 traceroute ipv6

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 *<ipv6-address|hostname>* parameter must be a valid IPv6 address or hostname. 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 range for *<port>* is zero (0) to 65535. The default value is 33434.

Default	port: 33434
Format	**traceroute ipv6** *<ipv6-address|hostname>* [**port** *<port>*]
Mode	Privileged EXEC

6.4.3 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 the current configuration on the switch to the default values. It does not reset the switch.

Format	**clear config**
Mode	Privileged EXEC

6.4.4 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

6.4.5 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

6.4.6 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

6.4.7 clear port-channel

This command clears all port-channels (LAGs).

Format `clear port-channel`
Mode Privileged EXEC

6.4.8 clear traplog

This command clears the trap log.

Format `clear traplog`
Mode Privileged EXEC

6.4.9 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format `clear vlan`
Mode Privileged EXEC

6.4.10 enable passwd

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case sensitive.

Format `enable passwd`
Mode Privileged EXEC

6.4.11 enable passwd encrypted *<password>*

This command allows the administrator to transfer the enable password between devices without having to know the password. The *<password>* parameter must be exactly 128 hexadecimal characters.

Format `enable passwd encrypted` *<password>*
Mode Privileged EXEC

6.4.12 enable password

Use this command to set a local password to control access to the privileged EXEC mode.

Format **enable password** *password* **[encrypted]**

Mode Privileged EXEC

Parameter	*Description*
password	Password for this level. Range: 8-64 characters.
encrypted	Encrypted password entered, copied from another switch configuration.

Example: The following example defines password `xxxyyyzzz` to control access to user and privilege levels.

```
(Broadcom FASTPATH Routing)# enable password xxxyyyzzz
```

6.4.12.1 no enable password

Use this command to remove the password requirement.

6.4.13 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

6.4.14 ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces.

Default
- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format **ping** *<ipaddress|hostname>* **[count** *<count>***] [interval** *<interval>***] [size** *<size>***]**

Modes
- Privileged EXEC
- User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	*Description*
count	Use the **count** parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the *<ip-address>* field. The range for *<count>* is 1 to 15 requests.
interval	Use the **interval** parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.

Parameter	Description
size	Use the **size** parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

Example: The following are examples of the CLI command.

Example: ping success:

```
(Broadcom FASTPATH Routing) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:

Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

Example: ping failure:

In Case of Unreachable Destination:

```
(Broadcom FASTPATH Routing) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

In Case Of Request TimedOut:

```
(Broadcom FASTPATH Routing) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

6.4.15 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

6.4.16 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

6.4.17 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 Priviledged EXEC

Value-types are:

Value-type	*Description*
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

6.4.18 reload fast

The reload command is used to initiate a switch management restart via reset of the system. The reload fast command will just do a clear config and will then re-apply the startup-config file.

Format **reload fast**

Mode Priviledged EXEC

6.4.19 copy

The **copy** command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (*image1* and *image2*) on the file system. Upload and download files from a server by using TFTP.

Format **copy** *<source> <destination>*

Mode Privileged EXEC

Replace the *<source>* and *<destination>* parameters with the options in Table 1. For the *<url>* source or destination, use :

*{tftp://<ipaddr|hostname>|<ip6address|*hostname*>/<filepath>/<filename>* [noval]*>*

For TFTP, SFTP and SCP, the *<ipaddr|hostname>* parameter is the IP address or host name of the server, *<filepath>* is the path to the file, and *<filename>* is the name of the file you want to upload or download. For SFTP and SCP, the <username> parameter is the username for logging into the remote server via SSH.

Note: *<ip6address>* is also a valid parameter for routing packages that support IPv6.

Caution! Remember to upload the existing fastpath.cfg file off the switch prior to loading a new release image in order to make a backup.

Table 1: Copy Parameters

Source	*Destination*	*Description*
nvram:backup-config	*nvram:startup-config*	Copies the backup configuration to the startup configuration.
nvram:clibanner	*<url>*	Copies the CLI banner to a server.
nvram:errorlog	*<url>*	Copies the error log file to a server.
nvram:fastpath.cfg	*<url>*	Uploads the binary config file to a server.
nvram:log	*<url>*	Copies the log file to a server.
nvram:oslog	*<url>*	Copies the OS system log file to a server
nvram:all-config	*<url>*	Contains a collection of different configuration files. This file is a “tar.gz” file and is generated with all files in the directories “/mnt/fastpath” and “/mnt/os” and important bootloader settings.
nvram:script <scriptname>	*<url>*	Copies a specified configuration script file to a server.
nvram:startup-config	*nvram:backup-config*	Copies the startup configuration to the backup configuration.
nvram:startup-config	*<url>*	Copies the startup configuration to a server.
nvram:startup-config	*nvram:file*	Copies startup config to specified file.
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:fastpath.cfg*	Downloads the binary config file 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 7.4 “Secure Shell Commands“ on page 7 - 9.
<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.
<url>	*nvram:all-config*	Downloads the gezipped collection of configuration files to the system.

Table 1: Copy Parameters (Continued)

Source	*Destination*	*Description*
<url>	pld	Downloads and updates PLD firmware. This needs time. While running some progress information is displayed. The PLD update is active only after a power-cycle.
<url>	*nvram:sslpem-dhstrong*	Downloads Secure DH Strong PEM file by sftp, scp or tftp
<url>	*nvram:sslpem-dhweak*	Downloads Secure DH Weak PEM file by sftp, scp or tftp.
<url>	*nvram:sslpem-root*	Downloads Secure Root PEM file by sftp, scp or tftp.
<url>	*nvram:sslpem-server*	Downloads Secure Server PEM file by sftp, scp or tftp
<url>	*fru-data*	This command downloads FRU data.
<url>	*{image1 | image2}*	Download an image from the remote server to either image.
image1	*image2*	Copy **image1** to **image2**.
image2	*image1*	Copy **image2** to **image1**.

6.4.20 copy ipmi-hpm

This command downloads an IPMI firmware image in HPM.1 format and remotely updates IPMI devices. If the flash process is interrupted or fails, the IPMC will automatically recover and use the previously installed image.

Format **copy** *tftp://<ipaddress>/<filename>* **ipmi-hpm** *{amc1..12 | pm1..4 | fan1..2}*

Mode Priviledged EXEC

6.4.21 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 Priviledged EXEC

6.4.21.1 no set bootstopkey

This command resets the bootstop key. The boot process can not be interrupted.

Format **no set bootstopkey**

Mode Priviledged EXEC

6.4.22 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 Priviledged EXEC

6.4.23 set watchdog

This command enables or disabled the system watchdog..

Format **`set watchdog`** *{ enable| disable}*

Mode Priviledged EXEC

6.4.24 show boardinfo post-status

This command displays the power on self test status of the board. It checks the status of the system selftest and the IPMC selftest.

Format **`show boardinfo post-status [system | ipmi]`**

Mode Priviledged EXEC

6.4.25 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 Priviledged EXEC

Note: It might take a while to get an output of the *"show boardinfo sensors brief"* command

6.4.26 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 Priviledged EXEC

Note: It might take a while to get an output of the *"show boardinfo event-log list"* command

6.4.27 show boardinfo update-status

This command displays the status of the firmware update process for the IPMI controller.

Format **`show boardinfo update-status`**

Mode Priviledged EXEC

6.4.28 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	Priviledged EXEC

Version information included

- Board name
- Base board serial number and part number
- Basic product identification (product number)
- IPMC firmware version
- IPMC boot block version
- System U-boot version
- System kernel version
- FASTPATH version
- CPLD revision
- FPGA version
- PHY 10G firmware version
- Base board broadcom silicon revision
- Processor CPU type
- Processor clock

Additionally software release information is displayed. This includes

- U-boot monitor and initialization release
- System kernel release
- System OS release
- IPMC firmware release
- FASTPATH release

6.4.29 show boardinfo address

This command displays the global address info of the board.

Format	**`show boardinfo address`**
Mode	Priviledged EXEC

6.4.30 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	Priviledged EXEC

6.4.31 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 Priviledged EXEC

6.4.32 set board time

This command sets the local time of the board. The format string is the same as for the UNIX date command (<month><day> <hours><minutes><Century><Year>.<seconds>).

Format `set boardinfo time` *<MMDDhhmmCCYY.ss>*

Mode Priviledged EXEC

6.4.33 show boardinfo time

This command displays the current date and time.

Format `show boardinfo time`

Mode Priviledged EXEC

6.4.34 show boardinfo memory-usage

This command displays the Memory Usage. It shows malloc and kernel statistics.

Format `show boardinfo memory-usage`

Mode Priviledged EXEC

6.4.35 show boardinfo cpu-load

This command displays the CPU load. It shows the total time, the user time, the system time and the idle time in current interval, 30 seconds interval and 5 minutes interval. All times are reported in percent.

Format `show boardinfo cpu-load`

Mode Priviledged EXEC

6.4.36 set board root-password

This command changes the current LINUX root password. The user will be asked by a prompt to specify the password and to reconfirm it a second time. An empty password can be specified by simply type <CR>. Then any password may be specified for the login. The factory password can be reconfigured (parameter ‘factory’).

Format `set board root-password [factory]`

Mode Priviledged EXEC

6.4.37 set board snmp ipmi-trap

This command enables/disables the generation of IPMI traps. If enabled, IPMI traps are sent for all SEL entries if no filter exists (see below) or for these entries for which an enabled filter rule fits.

Format	**`set board snmp ipmi-trap {enable | disable}`**
Mode	Priviledged EXEC

6.4.38 set board snmp filter

This command specified filter rules used if trap generation is enabled (see above). 20 rules can be specified. If you invoke this command you reach the “IPMI-filter Exec” mode. Use “exit” to leave this mode again. To keep the rule but disable it, you must specify “disable” in the “IPMI-filter Exec” mode.

Format	**`set board snmp filter`** *`<1..20>`*
Mode	Priviledged EXEC

6.4.38.1 no set board snmp filter

The “no” command can be used to delete a filter again. To keep the rule but disable it, you must specify “disable” in the “IPMI-filter Exec” mode.

Format	**`no set board snmp filter`** *`<1..20>`*
Mode	Priviledged EXEC

6.4.39 enable (filter)

This command enables the filter rule.

Format	**`enable`**
Mode	IPMI-filter Exec

6.4.40 disable (filter)

This command disables the filter rule. The rule is not deleted. The rule is disabled by default if a new rule is generated.

Format	**`disable`**
Mode	IPMI-filter Exec

6.4.41 ipmb (filter)

This command specifies the site for which a trap should be sent. The site is either ‘all’ for all sites (default) or ‘local’ for the local site or an IPMB address for remote sites. The IPMB address can be either specified decimal or hexadecimal (prefix ‘0x’).

Format	**`ipmb { all | local |`** *`<ipmb-address>`***`}`**
Mode	IPMI-filter Exec

6.4.42 type (filter)

This command specifies the sensor type for which a trap should be sent. The type is either ‘all’ for all types (default) or a pre-defined sensor type (by related name) or a value (decimal or hexadecimal).

Format **type {all | analog | discrete | temperature | voltage | current | fan | *<value>*}**

Mode IPMI-filter Exec

6.4.43 status (filter)

This command specifies the state for which a trap should be sent. Relevant only for analog sensors. The state is either ‘all’ for all states (default) or a special state.

Format **status {all | non-critical | critical | non-revoverable}**

Mode IPMI-filter Exec

6.4.44 assert (filter)

This command specifies if a trap should be sent for assert or deassert event. This can be used for discrete and analog sensors. For analog sensors assert means going low for lower thresholds and going high for upper thresholds. The assertion is either ‘all’ for all assertion states (default) or a special assertion state.

Format **assert {all | asserted | deasserted}**

Mode IPMI-filter Exec

6.4.45 show boardinfo snmp ipmi-trap

This command displays the configured values for generation of IPMI traps. It indicates the state (enable) of the IPMI trap generation as well as all generated filter rules.

Format **show boardinfo snmp ipmi-trap**

Mode Priviledged EXEC

6.5 Commands to configure startup services

This feature activates support for listing and configuring startup services. Services are board specific and defined by the BSP.

The commands invoke the /opt/kontron/bin/chkconfig utility directly.

6.5.1 set chkconfig

This command configures a BSP startup service.

Format **set chkconfig** *<service>*

Mode Priviledged EXEC

6.5.1.1 no set chkconfig

This command disables a BSP startup service.

Format	**no set chkconfig** *<service>*
Mode	Priviledged EXEC

Note that disabling basic services may make the system unusable, e.g. disabling syslogd or FASTPATH may make the system inaccessible.

6.5.2 show chkconfig

This command displays all currently installed services. Services are board specific and defined by the BSP.

Format	**show chkconfig**
Mode	Priviledged EXEC

6.6 Commands supporting SFP/SFP+ (AM4910 only)

The commands described in this chapter add support for SFP transceivers. Different types of transceivers are allowed to be used with the board.

Type	*Description*	*Implementation*	*Support*
1000BASE-SX	Short range, MMF, 850nm, 220-550m	Standard	YES
1000BASE-LX	Long range, SMF, 1310nm, 5km	Standard	YES
1000BASE-ZX	Long range, SMF, 1550nm, 70km (not standardized)	Standard	TBC
1000BASE-T	Copper SFP	Standard	YES

6.6.1 show sfp (AM4910 only)

This command displays information for a specified or all existing SFP's. The information is control/status information and/or the EEPROM data.

The show sfp {<slot/port> | all} mode command is only valid for 10G SFP+ interfaces and displays the operational mode.

Format	**show sfp** *<slot/port>* **show sfp** *<slot/port>* **detail** **show sfp** *<slot/port>* **mode** **show sfp all** **show sfp all mode**
Mode	Privileged EXEC

6.6.2 sfp mode (AM4910 only)

This command selects SFP operational mode for SFP+ modules. The mode may be 'autofw' to activate autodetect based on Broadcom PHY integrated firmware (default setting), 'autosw' to activate automatic detection by Broadcom supplied software modules or fixed configuration (10GBASE-LRM, standard, direct-attach cable or 1G-mode).

Format
```
sfp mode lrm
sfp mode standard
sfp mode da-cable
sfp mode mode-1g
sfp mode autofw
```

Mode Interface Mode

This allows using different types of transceivers.

Type	*Description*	*Support*	*SFP mode force command*
10GBASE-SR	Short range, MMF, 850nm, 65m	YES	sfp mode standard
10GBASE-LR	Long Range, SMF, 1310nm, 10km	YES	sfp mode standard
10GBASE-LRM	Long Range, MMF, 1310nm, 300m	YES	sfp mode lrm
10GBASE-ER	Extended Range, SMF, 40km	YES	sfp mode standard
10GBASE-SW	WAN mode, Short range, MMF, 850nm, 65m	NO	
10GBASE-LW	WAN mode, Long Range, SMF, 1310nm, 10km	NO	
10GBASE-EW	WAN mode, Extended Range, SMF, 40km	NO	

Mode	*Auto-Negotiation*	*Speed*	*CLI command*	*SFP mode force command*
1000BASE-X	IEEE 802.1D Clause 37	1000	auto-negotiate Note: advertise command is not supported on SFP+ transceiver based interfaces (not sgmii mode, no half-duplex operation)	sfp mode standard
1000BASE-X	none	1000	speed 1000, no auto-negotiate (Note: auto-negotiate will be turned off for speed 1000 forced mode)	sfp mode standard
10GBASE-X	none	10000	speed 10000, no auto-negotiate (Note: auto-negotiate will be turned off for speed 10000)	see Table above

6.7 Simple Network Time Protocol Commands

This section describes the commands you use to automatically configure the system time and date by using Simple Network Time Protocol (SNTP).

6.7.1 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

6.7.1.1 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

6.7.2 sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Multicast: For multicast mode the SNTP multicast address must be defined as a route to a device. This is set automatically to the network device (if networkport is specified) or serviceport device (if serviceport is specified). If deleting multicast mode the route is automatically deleted too.

Default	disabled
Format	**sntp client mode** *[broadcast | unicast | multicast]*
Mode	Global Config

6.7.2.1 no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format	**no sntp client mode**
Mode	Global Config

6.7.3 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

6.7.3.1 no sntp client port

This command resets the SNTP client port back to its default value.

Format	**no sntp client port**
Mode	Global Config

6.7.4 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

6.7.4.1 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

6.7.5 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

6.7.5.1 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

6.7.6 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

6.7.6.1 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

6.7.7 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 10.

Default 6

Format **sntp multicast client poll-interval** *<poll-interval>*

Mode Global Config

6.7.7.1 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

6.7.8 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|hostname> [<priority> [<version> [<portid>]]]*

Mode Global Config

6.7.8.1 no sntp server

This command deletes an server from the configured SNTP servers.

Format **no sntp server remove** *<ipaddress|hostname>*

Mode Global Config

6.7.9 show sntp

This command is used to display SNTP settings and status.

Format **show sntp**

Mode Privileged EXEC

Term	*Definition*
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.

6.7.10 show sntp client

This command is used to display SNTP client settings.

Format `show sntp client`

Mode Privileged EXEC

Term	*Definition*
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.

6.7.11 show sntp server

This command is used to display SNTP server settings and configured servers.

Format `show sntp server`

Mode Privileged EXEC

Term	*Definition*
Server IP Address / Hostname	IP address or hostname 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:

Term	*Definition*
IP Address / Hostname	IP address or hostname 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.

Term	Definition
Failed Unicast Requests	Number of failed requests from server.

6.7.12 clear board event-log

This command deletes all event-log records

Format `clear board event-log`

Mode Priviledged EXEC

6.7.13 show logging errcounter

This command displays the trace of the error counters.

Format `show logging errcounter`

Mode Priviledged EXEC

6.7.14 clear errcounter

This command clears the error counters trace.

Format `clear errcounter`

Mode Priviledged EXEC

6.7.15 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`

Mode Priviledged EXEC

6.8 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.

6.8.1 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

6.8.1.1 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

6.8.2 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

6.8.2.1 no client-identifier

This command deletes the client identifier.

Format **no client-identifier**
Mode DHCP Pool Config

6.8.3 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

6.8.3.1 no client-name

This command removes the client name.

Format **no client-name**
Mode DHCP Pool Config

6.8.4 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

6.8.4.1 no default-router

This command removes the default router list.

Format `no default-router`
Mode DHCP Pool Config

6.8.5 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

6.8.5.1 no dns-server

This command removes the DNS Server list.

Format `no dns-server`
Mode DHCP Pool Config

6.8.6 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

6.8.6.1 no hardware-address

This command removes the hardware address of the DHCP client.

Format `no hardware-address`
Mode DHCP Pool Config

6.8.7 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

6.8.7.1 no host

This command removes the IP address of the DHCP client.

Format **no host**
Mode DHCP Pool Config

6.8.8 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 23. *Minutes* is an integer from 0 to 59.

Default 1 (day)
Format **lease** *[{<days> [<hours>] [<minutes>] | infinite}]*
Mode DHCP Pool Config

6.8.8.1 no lease

This command restores the default value of the lease time for DHCP Server.

Format **no lease**
Mode DHCP Pool Config

6.8.9 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

6.8.9.1 no network

This command removes the subnet number and mask.

Format **no network**
Mode DHCP Pool Config

6.8.10 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

6.8.10.1 no bootfile

This command deletes the boot image name.

Format	**no bootfile**
Mode	DHCP Pool Config

6.8.11 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

6.8.11.1 no domain-name

This command removes the domain name.

Format	**no domain-name**
Mode	DHCP Pool Config

6.8.12 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

6.8.12.1 no netbios-name-server

This command removes the NetBIOS name server list.

Format	**no netbios-name-server**
Mode	DHCP Pool Config

6.8.13 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

6.8.13.1 no netbios-node-type

This command removes the NetBIOS node Type.

Format **no netbios-node-type**

Mode DHCP Pool Config

6.8.14 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

6.8.14.1 no next-server

This command removes the boot server list.

Format **no next-server**

Mode DHCP Pool Config

6.8.15 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

6.8.15.1 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

6.8.16 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

6.8.16.1 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

6.8.17 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

6.8.17.1 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

6.8.18 service dhcp

This command enables the DHCP server.

Default disabled

Format **`service dhcp`**

Mode Global Config

6.8.18.1 no service dhcp

This command disables the DHCP server.

Format **`no service dhcp`**

Mode Global Config

6.8.19 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

6.8.19.1 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

6.8.20 ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default enabled
Format **`ip dhcp conflict logging`**
Mode Global Config

6.8.20.1 no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format **`no ip dhcp conflict logging`**
Mode Global Config

6.8.21 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

6.8.22 clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format **`clear ip dhcp server statistics`**
Mode Privileged EXEC

6.8.23 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

6.8.24 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

Term	*Definition*
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.

6.8.25 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

Term	*Definition*
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.

6.8.26 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

Field	Definition
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:

Field	Definition
Network	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Field	Definition
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.

6.8.27 show ip dhcp server statistics

This command displays DHCP server statistics.

Format `show ip dhcp server statistics`

Modes
- Privileged EXEC
- User EXEC

Field	Definition
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:

Message	Definition
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:

Message	*Definition*
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.

6.8.28 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

Term	*Definition*
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.

6.9 DNS Client Commands

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components of FASTPATH.

6.9.1 ip domain lookup

Use this command to enable the DNS client.

Default enabled

Format `ip domain lookup`

Mode Global Config

6.9.1.1 no ip domain lookup

Use this command to disable the DNS client.

Format `no ip domain lookup`

Mode Global Config

6.9.2 ip domain name

Use this command to define a default domain name that FASTPATH software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. <*name*> may

not be longer than 255 characters and should not include an initial period. This <*name*> should be used only when the default domain name list, configured using the **ip domain list command,** is empty.

Default none

Format **ip domain name** *<name>*

Mode Global Config

Example: The CLI command **ip domain name yahoo.com** will configure yahoo.com as a default domain name. For an unqualified hostname xxx, a DNS query is made to find the IP address corresponding to xxx.yahoo.com.

6.9.2.1 no ip domain name

Use this command to remove the default domain name configured using the **ip domain name** command.

Format **no ip domain name**

Mode Global Config

6.9.3 ip domain list

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the **ip domain name** command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default none

Format **ip domain list** *<name>*

Mode Global Config

6.9.3.1 no ip domain list

Use this command to delete a name from a list.

Format **no ip domain list** *<name>*

Mode Global Config

6.9.4 ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter *<server-address>* is a valid IP address of the server. The preference of the servers is determined by the order they were entered.

Format **ip name-server <***server-address1***> [***server-address2...server-address8***]**

Mode Global Config

6.9.4.1 no ip name server

Use this command to remove a name server.

Format **no ip name-server [***server-address1...server-address8***]**

Mode Global Config

6.9.5 ip host

Use this command to define static host name-to-address mapping in the host cache. <*name*> is host name. <*ip address*> is the IP address of the host.

Default none

Format **ip host <*name*> <*ipaddress*>**

Mode Global Config

6.9.5.1 no ip host

Use this command to remove the name-to-address mapping.

Format **no ip host <*name*>**

Mode Global Config

6.9.6 ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The parameter <*number*> indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Default 2

Format **ip domain retry <*number*>**

Mode Global Config

6.9.6.1 no ip domain retry

Use this command to return to the default.

Format **no ip domain retry <*number*>**

Mode Global Config

6.9.7 ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter <*seconds*> specifies the time, in seconds, to wait for a response to a DNS query. <*seconds*> ranges from 0 to 3600.

Default 3

Format **ip domain timeout <*seconds*>**

Mode Global Config

6.9.7.1 no ip domain timeout

Use this command to return to the default setting.

Format **no ip domain timeout <*seconds*>**

Mode Global Config

6.9.8 clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format `clear host {<name> | all}`

Mode Privileged EXEC

Field	*Description*
name	A particular host entry to remove. <*name*> ranges from 1-255 characters.
all	Removes all entries.

6.9.9 show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. <*name*> ranges from 1-255 characters.

Format `show hosts [name]`

Mode User EXEC

Field	*Description*
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.
Number of Retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry Timeout Period	Amount of time to wait for a response to a DNS query.
Name Servers	Configured name servers.

Example: The following shows example CLI display output for the command.

```
<Broadcom FASTPATH SWITCHING> show hosts

Host name..................... Device
Default domain................ gm.com
Default domain list........... yahoo.com, Stanford.edu, rediff.com
Domain Name lookup............ Enabled
Number of retries............. 5
Retry timeout period.......... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19


Configured host name-to-address mapping:

Host                          Addresses
----------------------------- -------------------------------
```

```
accounting.gm.com              176.16.8.8

Host              Total   Elapsed      Type       Addresses
---------------- -------- ------     --------      --------------
www.stanford.edu    72       3          IP        171.64.14.203
```

6.10 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.

6.10.1 debug arp

Use this command to enable ARP debug protocol messages.

Default disabled

Format **`debug arp`**

Mode Privileged EXEC

6.10.1.1 no debug arp

Use this command to disable ARP debug protocol messages.

Format **`no debug arp`**

Mode Privileged EXEC

6.10.2 debug auto-voip

Use this command to enable Auto VOIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Default disabled

Format **`debug auto-voip`** *`[H323|SCCP|SIP]`*

Mode Privileged EXEC

6.10.2.1 no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format **`no debug auto-voip`**

Mode Privileged EXEC

6.10.3 debug clear

This command disables all previously enabled “debug” traces.

Default disabled

Format `debug clear`
Mode Privileged EXEC

6.10.4 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

6.10.4.1 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

6.10.5 debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default disabled
Format `debug dot1x`
Mode Privileged EXEC

6.10.5.1 no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format `no debug dot1x`
Mode Privileged EXEC

6.10.6 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

6.10.6.1 no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format `no debug igmpsnooping packet`

Mode Privileged EXEC

6.10.7 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:

Parameter	*Definition*
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
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.

6.10.7.1 no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format **no debug igmpsnooping transmit**

Mode Privileged EXEC

6.10.8 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:

Parameter	*Definition*
RX	A packet received by the device.
Intf	The interface that the packet went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
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.

6.10.8.1 no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format **`no debug igmpsnooping receive`**

Mode Privileged EXEC

6.10.9 debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default disabled

Format **`debug lacp packet`**

Mode Privileged EXEC

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
```

6.10.9.1 no debug lacp packet

This command disables tracing of LACP packets.

Format `no debug lacp packet`
Mode Privileged EXEC

6.10.10 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:

Parameter	*Definition*
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 unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
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.

6.10.10.1 no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format `no debug ping packet`
Mode Privileged EXEC

6.10.11 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

6.10.11.1 no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format `no debug spanning-tree bpdu`

Mode Privileged EXEC

6.10.12 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:

Parameter	*Definition*
RX	A packet received by the device.
Intf	The interface that the packet came in on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
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.

6.10.12.1 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

6.10.13 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:

Parameter	*Definition*
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
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.

6.10.13.1 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

6.10.14 logging persistent

Use this command to configure the Persistent logging for the switch. The severity level of logging messages is specified at severity level. Possible values for severity level are *(emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).*

Default	Disable
Format	**logging persistent** *<severity level>*
Mode	Global Config

6.10.14.1 no logging persistent

Use this command to disable the persistent logging in the switch.

Format	**no logging persistent**
Mode	Global Config

6.11 Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.

Note: The cable test feature is supported only for copper cable. It is not supported for optical fiber cable.

If the port has an active link while the cable test is run, the link can go down for the duration of the test.

6.11.1 cablestatus

This command returns the status of the specified port.

Format **cablestatus <***slot/port***>**

Mode Privileged EXEC

Field	*Description*
Cable Status	One of the following statuses is returned: • **Normal**: The cable is working correctly. • **Open**: The cable is disconnected or there is a faulty connector. • **Short**: There is an electrical short in the cable. • **Cable Test Failed**: The cable status could not be determined. The cable may in fact be working.
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

6.12 sFlow Commands

sFlow® is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

6.12.1 sflow receiver

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

6.12.1.1 no sflow receiver

Use this command to set the sFlow collector parameters back to the defaults.

Format **no sflow receiver** *<indx> {ip <ip-address> | maxdatagram <size> | owner <string> timeout <interval> | port <14-port>}*

Mode Global Config

6.12.2 sflow sampler

A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance for this data source if *<rcvr_idx>* is valid.

6.12.2.1 no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

6.12.3 sflow poller

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance for this data source if <*rcvr_idx*> is valid.

6.12.3.1 no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

6.12.4 show sflow agent

The sFlow agent collects time-based sampling of network interface statistics and flow-based samples. These are sent to the configured sFlow receivers. Use this command to display the sFlow agent information.

Example: The following shows example CLI display output for the command.

```
(switch) #show sflow agent

sFlow Version..................................... 1.3;Broadcom Corp;1.0
IP Address........................................ 10.131.12.66
```

show sflow pollers

Use this command to display the sFlow polling instances created on the switch. Use “-” for range.

6.12.5 show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

Example: The following shows example CLI display output for the command.

```
(switch) #show sflow receivers 1
Receiver Index.................................... 1
Owner String.....................................
Time out.......................................... 0
IP Address:....................................... 0.0.0.0
Address Type...................................... 1
Port.............................................. 6343
Datagram Version.................................. 5
Maximum Datagram Size............................. 1400
```

6.12.6 show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

6.13 AutoInstall Commands

The AutoInstall feature enables the automatic configuration of a switch when the device is initialized and no configuration file is found on the switch. When no configuration file is found, it is downloaded from a TFTP server and saved to non-volatile memory. The TFTP server name or address is provided by a DHCP server in response to a IP address request initiated during startup.

6.13.1 boot autoinstall

The command enables/disables autoinstall on the switch.

Default `enable`

Format `boot autoinstall {start | stop}`

Mode Privileged EXEC

6.13.2 boot autoinstall auto-save

This command enables or disables saving the network configuration to non-volatile memory. When enabled, the configuration is saved after downloading from the TFTP server without operator intervention. When disabled, the operator must explicitly save the configuration, if needed.

Default `enable`

Format `boot autoinstall auto-save`

Mode Privileged EXEC

6.13.2.1 no boot autoinstall auto-save

This command disables saving the network configuration to non-volatile memory.

6.13.3 boot autoinstall retry-count

This command sets the number of unicast TFTP attempts for the configuration file.

Default `3`

Format `boot autoinstall retry-count <1-6>`

Mode Privileged EXEC

6.13.3.1 no boot autoinstall retry-count

This command sets to the default the number of unicast TFTP attempts for the configuration file.

Format `no boot autoinstall retry-count`

Mode Privileged EXEC

6.13.4 show autoinstall

This command displays the current status of the AutoInstall process.

Format `show autoinstall`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(switch) #show autoinstall

AutoInstall Mode.............................. Started
AutoSave Mode................................. Enabled
AutoInstall Retry Count....................... 3
AutoInstall State............................. Waiting for boot options
```

Chapter 7

Management Commands

7. Management Commands

This chapter describes the management commands available in the FASTPATH CLI.

The Management Commands chapter contains the following sections:

- 7.1 “Network Interface Commands” on page 7 - 2
- 7.2 “Console Port Access Commands” on page 7 - 6
- 7.3 “Telnet Commands” on page 7 - 7
- 7.4 “Secure Shell Commands” on page 7 - 9
- 7.5 “Management Security Commands” on page 7 - 11
- 7.6 “Hypertext Transfer Protocol Commands” on page 7 - 12
- 7.7 “Access Commands” on page 7 - 18
- 7.8 “User Account Commands” on page 7 - 18
- 7.9 “SNMP Commands” on page 7 - 28
- 7.10 “RADIUS Commands” on page 7 - 39
- 7.11 “TACACS+ Commands” on page 7 - 50
- 7.12 “Configuration Scripting Commands” on page 7 - 53
- 7.13 “Pre-login Banner and System Prompt Commands” on page 7 - 54

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.

7.1 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 - 21

7.1.1 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

7.1.2 clicm

This command executes a specified CLI command on the CM. The arguments **must** be enclosed with quotes (e.g. `clicm “sensor show all”´). To get a list of available commands use `clicm “help”´.

Format	`clicm` *<arguments>*
Mode	Privileged EXEC

7.1.3 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

7.1.4 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

7.1.5 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

7.1.6 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

7.1.7 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

7.1.8 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

7.1.8.1 no network mac-type

This command resets the value of MAC address to its default.

Format **`no network mac-type`**

Mode Privileged EXEC

7.1.9 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. The network interface is always considered to be up, whether or not any member ports are up; therefore, the show network command will always show “Interface Status” as “Up”.

Format **`show network`**

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
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.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/ Length	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
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.

Term	Definition
MAC Address Type	The MAC address which 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 being used. The options are bootp | dhcp | none.

Example: The following shows example CLI display output for the network port.

```
(Ethernet Fabric) #show network

Interface Status.............................. Always Up
IP Address.................................... 10.250.3.1
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.250.3.3
Burned In MAC Address......................... 00:10:18:82:03:37
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Network Configuration Protocol Current........ None
Management VLAN ID............................ 1
```

7.1.10 show serviceport

This command displays service port configuration information.

Format **`show serviceport`**

Mode Privileged EXEC
User EXEC

Term	Definition
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.

Example: The following shows example CLI display output for the service port.

```
(Ethernet Fabric) #show serviceport

Interface Status.............................. Up
IP Address.................................... 10.230.3.51
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.230.3.1
ServPort Configured Protocol Current.......... DHCP
Burned In MAC Address......................... 00:A0:A5:5D:20:3C
```

7.2 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.

7.2.1 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

7.2.2 line

This command gives you access to the Line Console mode, which allows you to configure various Telnet settings and the console port, as well as to configure console login/enable authentication.

Format `line {console|telnet|ssh}`

Mode Global Config

Term	*Definition*
console	Console terminal line.
telnet	Virtual terminal for remote console access (Telnet).
ssh	Virtual terminal for secured remote console access (SSH).

Example: The following shows an example of the CLI command.

```
(Broadcom FASTPATH Routing)(config)#line telnet
(Broadcom FASTPATH Routing)(config-telnet)#
```

7.2.3 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

7.2.3.1 no serial baudrate

This command sets the communication rate of the terminal interface.

Format `no serial baudrate`

Mode Line Config

7.2.4 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

7.2.4.1 no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

Format `no serial timeout`

Mode Line Config

7.2.5 show serial

This command displays serial communication settings for the switch.

Format `show serial`

Modes
- Privileged EXEC
- User EXEC

Term	*Definition*
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.

7.3 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.

7.3.1 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

7.3.1.1 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

7.3.2 telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address or host name. 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 <ip-address|hostname> <port> [debug] [line] [noecho]`

Modes
- Privileged EXEC
- User EXEC

7.3.3 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

7.3.3.1 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

7.3.4 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

7.3.4.1 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

7.3.5 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

Term	*Definition*
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.

7.4 Secure Shell Commands

This section describes the commands you use to configure Secure Shell (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.

7.4.1 ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the **`ip ssh server enable`** command.)

Default disabled

Format `ip ssh`

Mode Privileged EXEC

7.4.2 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

7.4.3 ip ssh server enable

This command enables the IP secure shell server.

Default disabled

Format **`ip ssh server enable`**

Mode Privileged EXEC

7.4.3.1 no ip ssh server enable

This command disables the IP secure shell server.

Format **`no ip ssh server enable`**

Mode Privileged EXEC

7.4.4 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

7.4.4.1 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

7.4.5 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

7.4.5.1 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

7.4.6 show ip ssh

This command displays the ssh settings.

Format `show ip ssh`

Mode Privileged EXEC

Term	*Definition*
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.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

7.5 Management Security Commands

This section describes commands you use to generate keys and certificates, which you can do in addition to loading them as before.

7.5.1 crypto certificate generate

Use this command to generate self-signed certificate for HTTPS. The generate RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format `crypto certificate generate`

Mode Global Config

7.5.1.1 no crypto certificate generate

Use this command to delete the HTTPS certificate files from the device, regardless of whether they are self-signed or downloaded from an outside source.

Format `no crypto certificate generate`
Mode Global Config

7.5.2 crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format `crypto key generate rsa`
Mode Global Config

7.5.2.1 no crypto key generate rsa

Use this command to delete the RSA key files from the device.

Format `no crypto key generate rsa`
Mode Global Config

7.5.3 crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format `crypto key generate dsa`
Mode Global Config

7.5.3.1 no crypto key generate dsa

Use this command to delete the DSA key files from the device.

Format `no crypto key generate dsa`
Mode Global Config

7.6 Hypertext Transfer Protocol Commands

This section describes the commands you use to configure Hypertext Transfer Protocol (HTTP) and secure HTTP access to the switch. Access to the switch by using a Web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the Web.

7.6.1 ip http authentication

Use this command to specify authentication methods for http server users. The default configuration is the local user database is checked. This action has the same effect as the command **`ip http authentication local`**. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the

command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

Default `local`
Format `ip http authentication` *method1* [*method2*...]
Mode Global Config

Parameter	*Description*
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Example: The following example configures the http authentication.

```
(switch)(config)# ip http authentication radius local
```

7.6.1.1 no ip http authentication

Use this command to return to the default.

7.6.2 ip https authentication

Use this command to specify authentication methods for https server users. The default configuration is the local user database is checked. This action has the same effect as the command **`ip https authentication local`**. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

Default `local`
Format `ip https authentication` *method1* [*method2*...]
Mode Global Config

Parameter	*Description*
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Example: The following example configures https authentication.

```
(switch)(config)# ip https authentication radius local
```

7.6.2.1 no ip https authentication

Use this command to return to the default.

7.6.3 ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Default enabled
Format `ip http server`
Mode Privileged EXEC

7.6.3.1 no ip http server

This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Format `no ip http server`
Mode Privileged EXEC

7.6.4 ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

Default disabled
Format `ip http secure-server`
Mode Privileged EXEC

7.6.4.1 no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

Format `no ip http secure-server`
Mode Privileged EXEC

7.6.5 ip http java

This command enables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Default Enabled
Format `ip http java`
Mode Privileged EXEC

7.6.5.1 no ip http java

This command disables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Format `no ip http java`
Mode Privileged EXEC

7.6.6 ip http session hard-timeout

This command configures the hard timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite hard-timeout. When this timeout expires, the user will be forced to re-authenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default 24

Format **ip http session hard-timeout** *<0-168>*

Mode Privileged EXEC

7.6.6.1 no ip http session hard-timeout

This command restores the hard timeout for un-secure HTTP sessions to the default value.

Format **no ip http session hard-timeout**

Mode Privileged EXEC

7.6.7 ip http session maxsessions

This command limits the number of allowable un-secure HTTP sessions. Zero is the configurable minimum.

Default 16

Format **ip http session maxsessions** *<0-16>*

Mode Privileged EXEC

7.6.7.1 no ip http session maxsessions

This command restores the number of allowable un-secure HTTP sessions to the default value.

Format **no ip http session maxsessions**

Mode Privileged EXEC

7.6.8 ip http session soft-timeout

This command configures the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch.

Default 5

Format **ip http session soft-timeout** *<0-60>*

Mode Privileged EXEC

7.6.8.1 no ip http session soft-timeout

This command resets the soft timeout for un-secure HTTP sessions to the default value.

Format **no ip http session soft-timeout**

Mode Privileged EXEC

7.6.9 ip http secure-session hard-timeout

This command configures the hard timeout for secure HTTP sessions in hours. When this timeout expires, the user is forced to re-authenticate. This timer begins on initiation of the Web session and is unaffected by the activity level of the connection. The secure-session hard-timeout can not be set to zero (infinite).

Default 24

Format **ip http secure-session hard-timeout** *<1-168>*

Mode Privileged EXEC

7.6.9.1 no ip http secure-session hard-timeout

This command resets the hard timeout for secure HTTP sessions to the default value.

Format **no ip http secure-session hard-timeout**

Mode Privileged EXEC

7.6.10 ip http secure-session maxsessions

This command limits the number of secure HTTP sessions. Zero is the configurable minimum.

Default 16

Format **ip http secure-session maxsessions** *<0-16>*

Mode Privileged EXEC

7.6.10.1 no ip http secure-session maxsessions

This command restores the number of allowable secure HTTP sessions to the default value.

Format **no ip http secure-session maxsessions**

Mode Privileged EXEC

7.6.11 ip http secure-session soft-timeout

This command configures the soft timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, you are forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch. The secure-session soft-timeout can not be set to zero (infinite).

Default 5

Format **ip http secure-session soft-timeout** *<1-60>*

Mode Privileged EXEC

7.6.11.1 no ip http secure-session soft-timeout

This command restores the soft timeout for secure HTTP sessions to the default value.

Format **no ip http secure-session soft-timeout**

Mode Privileged EXEC

7.6.12 ip http secure-port

This command is used to set the SSL port where port can be 1-65535 and the default is port 443.

Default 443

Format **`ip http secure-port`** *<portid>*

Mode Privileged EXEC

7.6.12.1 no ip http secure-port

This command is used to reset the SSL port to the default value.

Format **`no ip http secure-port`**

Mode Privileged EXEC

7.6.13 ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Default SSL3 and TLS1

Format **`ip http secure-protocol`** *[SSL3] [TLS1]*

Mode Privileged EXEC

7.6.14 show ip http

This command displays the http settings for the switch.

Format **`show ip http`**

Mode Privileged EXEC

Term	*Definition*
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.
HTTP Session Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http sessions in minutes.
Certificate Present	Indicates whether the secure-server certificate files are present on the device.

Term	Definition
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

7.7 Access Commands

Use the commands in this section to close remote connections or to view information about connections to the system.

7.7.1 disconnect

Use the **disconnect** command to close Telnet or SSH sessions. Use *all* to close all active 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

7.7.2 show loginsession

This command displays current Telnet and serial port connections to the switch.

Format **show loginsession**

Mode Privileged EXEC

Term	Definition
ID	Login Session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote 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.
Session Type	Shows the type of session, which can be telnet, serial, or SSH.

7.8 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.

7.8.1 aaa authentication login

Use this command to set authentication at login. The default and optional list names created with the command are used with the `aaa authentication login` command. Create a list by entering the `aaa authentication login` *list-name method* command for a particular protocol, where *list-name* is any character string used to

name this list. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the fInal method in the command line. For example, if **none** is specified as an authentication method after **radius**, no authentication is used if the RADIUS server is down.

Default
- defaultList. Used by the console and only contains the method none.
- networkList. Used by telnet and SSH and only contains the method local.

Format aaa authentication login {default|*list-name*} *method1* [*method2*...]

Mode Global Config

Parameter	*Definition*
default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string of up to 12 characters used to name the list of authentication methods activated when a user logs in.
method1...[method 2...]	At least one from the following: • enable. Uses the enable password for authentication. • line. Uses the line password for authentication. • local. Uses the local username database for authentication. • none. Uses no authentication. • radius. Uses the list of all RADIUS servers for authentication. • tacacs. Uses the list of all TACACS servers for authentication.

Example: The following shows an example of the command.

```
(switch)(config)# aaa authentication login default radius local enable none
```

7.8.1.1 no aaa authentication login

This command returns to the default.

Format aaa authentication login {default|*list-name*}

Mode Global Config

7.8.2 aaa authentication enable

Use this command to set authentication for accessing higher privilege levels. The default enable list is enableList. It is used by console, telnet, and SSH and only contains the method none.

The default and optional list names created with the aaa authentication enable command are used with the enable authentication command. Create a list by entering the aaa authentication enable list-name method command where list-name is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line.

Note: Enable will not succeed for a level one user if no authentication method is defined. A level one user must authenticate to get to privileged EXEC mode. For example, if `none` is specified as an authentication method after radius, no authentication is used if the RADIUS server is down.

Note: Requests sent by the switch to a RADIUS server include the username `$enabx$`, where `x` is the requested privilege level. For enable to be authenticated on Radius servers, add `$enabx$` users to them. The login user ID is now sent to TACACS+ servers for enable authentication.

Default default

Format `aaa authentication enable {default|`*`list-name`*`} `*`method1`*` [`*`method2`*`...]`

Mode Global Config

Parameter	*Description*
default	Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
list-name	Character string used to name the list of authentication methods activated, when using access higher privilege levels. Range: 1-12 characters.
method1[method2...]	Specify at least one from the following: • `enable`. Uses the enable password for authentication. • `line`. Uses the line password for authentication. • `none`. Uses no authentication. • `radius`. Uses the list of all RADIUS servers for authentication. • `tacacs`. Uses the list of all TACACS+ servers for authentication.

Example: The following example sets authentication when accessing higher privilege levels.

```
(switch)(config)# aaa authentication enable default enable
```

7.8.2.1 no aaa authentication enable

Use this command to return to the default configuration.

Format `no aaa authentication enable {default|`*`list-name`*`}`

Mode Global Config

7.8.3 enable authentication

Use this command to specify the authentication method list when accessing a higher privilege level from a remote telnet or console.

Format `enable authentication {default|`*`list-name`*`}`

Mode Line Config

Parameter	*Description*
default	Uses the default list created with the **`aaa authentication enable`** command.
list-name	Uses the indicated list created with the **`aaa authentication enable`** command.

Example: The following example specifies the default authentication method when accessing a higher privilege level console.

```
(switch)(config)# line console
(switch)(config-line)# enable authentication default
```

7.8.3.1 no enable authentication

Use this command to return to the default specified by the **`enable authentication`** command.

Format `no enable authentication`

Mode Line Config

7.8.4 username

Use this command to add a new user to the local users database. The default privilege level is 1. This command can be used to unlock a locked user account for an alread existing user.

Format **`username`** *`name`* **`password`** *`password`* **`[level`** *`level`***`][encrypted]`**

Mode Global Config

Parameter	*Description*
name	The name of the user. Range: 1-32 characters.
password	The authentication password for the user. Range 8-64 characters. This value can be zero if the **`no passwords min-length`** command has been executed.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15. Enter access level 1 for Read Access or 15 for Read/Write Access.
encrypted	Encrypted password entered, copied from another switch configuration.

Example: The following example configures user `bob` with password `xxxyyymmmm` and user level 15.

```
(switch)(config)# username bob password xxxyyymmmm level 15
```

7.8.4.1 no username

Use this command to remove a user name.

7.8.5 username *name nopassword*

Use this command to remove an existing user's password (NULL password).

Format **`username`** *`name nopassword`* **`[level`** *`level`***`]`**

Mode Global Config

Parameter	*Description*
name	The name of the user. Range: 1-32 characters.
password	The authentication password for the user. Range 8-64 characters.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15.

7.8.6 username 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.

Defaults
- admin - readwrite
- other - readonly

Format **username snmpv3 accessmode** *<username> {readonly | readwrite}*

Mode Global Config

7.8.6.1 no username 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 username snmpv3 accessmode** *<username>*

Mode Global Config

7.8.7 username 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 **username snmpv3 authentication** *<username> {none | md5 | sha}*

Mode Global Config

7.8.7.1 no username 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 username snmpv3 authentication** *<username>*

Mode Global Config

7.8.7.2 username 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 **username snmpv3 encryption** *<username> {none | des[key]}*

Mode Global Config

7.8.7.3 no username 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 username snmpv3 encryption** *<username>*

Mode Global Config

7.8.8 username snmpv3 encryption encrypted

This command specifies the des encryption protocol and the required encryption key for the specified user. The encryption key must be 8 to 64 characters long.

Default no encryption

Format **username snmpv3 encryption encrypted** *<username>* **des** *<key>*

Mode Global Config

7.8.9 show users

This command displays the configured user names and their settings. The `show users` command displays truncated user names. Use the `show users long` command to display the complete usernames. The `show users` 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

Term	*Definition*
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.
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.

7.8.10 show users long

This command displays the complete usernames of the configured users on the switch.

Format `show users long`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(switch) #show users long
User Name
------------
admin
guest
test1111test1111test1111test1111
```

7.8.11 show users accounts

This command displays the local user status with respect to user account lockout and password aging.This command displays truncated user names. Use the `show users long` command to display the complete usernames.

Format `show users accounts`

Mode Privileged EXEC

Term	*Definition*
User Name	The local user account's user name.
Access Mode	The user's access level (read-only or read/write).
Lockout Status	Indicates whether the user account is locked out (true or false).
Password Expiration Date	The current password expiration date in date format.

Example: The following example diplays information about the local user database.

```
(switch)#show users accounts

UserName             Privilege Password Password     Lockout
                               Aging    Expiry date
-------------------- --------- -------- ------------ -------
admin                15        ---      ---          False
guest                1         ---      ---          False
```

7.8.12 show users login-history

Use this command to display information about the login history of users.

Format `show users login-history [long]`

Mode Privileged EXEC

Parameter	*Description*
name	Name of the user. Range: 1-20 characters.

Example: The following example shows user login history outputs.

```
Login Time            Username  Protocol  Location
--------------------  --------- --------- ---------------
Jan 19 2005 08:23:48  Bob       Serial
Jan 19 2005 08:29:29  Robert    HTTP      172.16.0.8
Jan 19 2005 08:42:31  John      SSH       172.16.0.1
Jan 19 2005 08:49:52  Betty     Telnet    172.16.1.7
```

7.8.13 login authentication

Use this command to specify the login authentication method list for a line (console, telnet, or SSH). The default configuration uses the default set with the command **`aaa authentication login`**.

Format **`login authentication {default|`***`list-name`***`}`**

Mode Line Configuration

Parameter	*Description*
default	Uses the default list created with the **`aaa authentication login`** command.
list-name	Uses the indicated list created with the **`aaa authentication login`** command.

Example: The following example specifies the default authentication method for a console.

```
(switch) (config)# line console
(switch) (config-line)# login authentication default
```

7.8.13.1 no login authentication

Use this command to return to the default specified by the **`authentication login`** command.

7.8.14 passwd

This command allows the currently logged in user to change his or her password without having read/write privileges.

Format **`password`** *<cr>*

Mode User EXEC

7.8.15 password (Line Configuration)

Use this command to specify a password on a line. The default configuration is no password is specified.

Format **`password`** *password* **`[encrypted]`**

Mode Line Config

Parameter	*Definition*
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration.

Example: The following example specifies a password `mcmxxyyy` on a line.

```
(switch)(config-line)# password mcmxxyyy
```

7.8.15.1 no password (Line Configuration)

Use this command to remove the password on a line.

7.8.16 password (User EXEC)

Use this command to allow a user to change the password for only that user. This command should be used after the password has aged. The user is prompted to enter the old password and the new password.

Format	**password**
Mode	User EXEC

Example: The following example shows the prompt sequence for executing the password command.

```
(switch)>password
Enter old password:********
Enter new password:********
Confirm new password:********
```

7.8.17 passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 8-64.

Default	8
Format	**passwords min-length** *<8-64>*
Mode	Global Config

7.8.17.1 no passwords min-length

Use this command to set the minimum password length to the default value.

Format	**no passwords min-length**
Mode	Global Config

7.8.18 passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don't reuse their passwords often. The valid range is 0-10.

Default	0
Format	**passwords history** *<0-10>*
Mode	Global Config

7.8.18.1 no passwords history

Use this command to set the password history to the default value.

Format `no passwords history`
Mode Global Config

7.8.19 passwords aging

Use this command to implement aging on passwords for local users. When a user's password expires, the user will be prompted to change it before logging in again. The valid range is 1-365. The default is 0, or no aging.

Default 0
Format `passwords aging` *<1-365>*
Mode Global Config

7.8.19.1 no passwords aging

Use this command to set the password aging to the default value.

Format `no passwords aging`
Mode Global Config

7.8.20 passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can re-activate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

Default 0
Format `passwords lock-out` *<1-5>*
Mode Global Config

7.8.20.1 no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format `no passwords lock-out`
Mode Global Config

7.8.21 show passwords configuration

Use this command to display the configured password management settings.

Format `show passwords configuration`
Mode Privileged EXEC

Term	*Definition*
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.

7.8.22 write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running config nvram:startup-config`.

Format **`write memory`**

Mode Privileged EXEC

7.9 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.

7.9.1 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

7.9.2 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

7.9.2.1 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

7.9.3 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

7.9.3.1 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

7.9.4 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

7.9.4.1 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

7.9.5 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

7.9.5.1 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

7.9.6 snmp-server community ro

Format **`snmp-server community ro`** *<name>*

Mode Global Config

This command restricts access to switch information. The access mode is read-only (also called public).

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

7.9.7 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 2.7 “Protected Ports Commands” on page 2 - 37.

Default disabled

Format **`snmp-server enable traps violation`**

Mode Interface Config

7.9.7.1 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

7.9.8 snmp-server enable traps

This command enables the Authentication Flag.

Default enabled
Format `snmp-server enable traps`
Mode Global Config

7.9.8.1 no snmp-server enable traps

This command disables the Authentication Flag.

Format `no snmp-server enable traps`
Mode Global Config

7.9.9 snmp-server enable traps all

This command enables all SNMP trap groups which can be displayed by "`show trapflags`".

Format `snmp-server enable traps all`
Mode Priviledged Exec

7.9.9.1 no snmp-server enable traps all

This command disables all SNMP trap groups which can be displayed by "`show trapflags`".

Format `no snmp-server enable traps all`
Mode Priviledged Exec

7.9.10 snmp-server enable traps linkmode

Note: This command may not be available on all platforms.

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 7 - 34.

Default enabled
Format `snmp-server enable traps linkmode`
Mode Global Config

7.9.10.1 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

7.9.11 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

7.9.11.1 no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format `no snmp-server enable traps multiusers`
Mode Global Config

7.9.12 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

7.9.12.1 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

7.9.13 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. The SNMP trap address can be set using both an IPv4 address format as well as an IPv6 global address format.

Example: The following shows an example of the CLI command.

```
(admin #) snmptrap mytrap ip6addr 3099::2
```

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

7.9.13.1 no snmptrap

This command deletes trap receivers for a community.

Format **no snmptrap** *<name> <ipaddr>*

Mode Global Config

7.9.14 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

7.9.15 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

7.9.16 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

7.9.16.1 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

7.9.17 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 7 - 31.

Format **snmp trap link-status**

Mode Interface Config

7.9.17.1 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

7.9.18 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 7 - 31.

Format **snmp trap link-status all**

Mode Global Config

7.9.18.1 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 7 - 31.

Format **no snmp trap link-status all**

Mode Global Config

7.9.19 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

Term	*Definition*
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.

7.9.20 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

Term	*Definition*
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 IPv4 address to receive SNMP traps from this device.
IPv6 Address	The IPv6 address to receive SNMP traps from this device.
SNMP Version	SNMPv2
Mode	The receiver's status (enabled or disabled).

Example: The following shows an example of the CLI command.

```
(admin) #show snmptrap

 Community Name    IpAddress      IPv6 Address      Snmp Version     Mode
   Mytrap          0.0.0.0         2001::1          SNMPv2          Enable show trapflags
```

7.9.21 show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 and OSPFv3 trapflags. 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

Term	*Definition*
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.
Broadcast Storm Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether broadcast storm traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)
DVMRP Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPF traps' information.
OSPFv3 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPFv3 trap flags are not enabled, then the command displays *disabled*. Otherwise, the command shows all the enabled OSPFv3 traps' information.
PIM Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.

7.9.22 snmptrap

This command adds an SNMP 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. The SNMP trap address can be set using both an IPv4 address format as well as an IPv6 global address format.

Example: The following shows an example of the CLI command.

```
(admin #) snmptrap mytrap ip6addr 3099::2
```

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.”

The notification argument specifies the type (trap or inform request) for generating traps. The default is ‘trap’. The ‘inform request’ is only possible for version 2c. This is implicitely set by specifying ‘inform request’.

Format **snmptrap** *<name>* **ipaddr** *<ipaddr>*
snmptrap *<name>* **ipaddr** *<ipaddr>* **snmpversion** *{snmpv1 | snmpv2}*
snmptrap *<name>* **ipaddr** *<ipaddr>* **notification** *{trap | inform}*

Mode Global Config

7.9.22.1 no snmptrap

This command deletes trap receivers for a community.

Format **no snmptrap** *<name> <ipaddr>*
no snmptrap mode *<name> <ipaddr>*

Mode Global Config

7.9.23 snmptrap notification

This command specifies the notification type (trap or inform request) for generating traps. The default is ‘trap’. The ‘inform request’ is only possible for version 2c. The version is not checked, but setting ‘inform request’ for version 1 means that the trap is sent as ‘trap’ anyway.

Format **snmptrap notification** *<name> <ipaddr> {trap | inform}*

Mode Global Config

7.9.24 snmp-server engine-id

This command configures the algorithm used to generate the Snmp-Engine-ID. This object is used only in SNMPv3. The algorithm should generate a unique ID (see RFC 3411). It can be selected a RFC 3411 defined algorithm containing the MAC address (mac), a specified IP address (ip) or a specified text (text). It may be also selected a simple enterprise specific algorithm (simple) containing the SNMP port (161). Note that this algorithm is not unique. Default is the RFC 3411 related algorithm with MAC address (mac).

A new configured algorithm will become effective not before the system has been rebooted because the Snmp-Engine-ID is used also to encrypt the community and user passwords. Therefore the user have to save the configuration and reboot the system to activate the new algorithm..

Format **snmp-server engine-id** *{mac | ip <ip-addr> | text <text> | simple}*

Mode Global Config

7.9.25 show snmp-engine-id

This command displays the algorithm used to generate the Snmp-Engine-ID. It displays the configured and the currently active algotithm. A configured algorithm will become active after the next system reboot..

Format `show snmp-engine-id`

Mode Privileged Exec

7.9.26 set board snmp site

This command configures the sites used to monitor IPMI information via SNMP. The parameter 'local' specifies the local site, remote sites must be specified by the related IPMB address. The IPMB address can be specified decimal or hexadecimal (prefix '0x').
If the IPMI SEL is full no more SEL entries are stored. This effects that for monitoring and setting traps no more traps are generated. If adding the parameter 'sel-clear' the SEL is cleared automatically if the specified limit (see 'set board snmp sel-clear limit' below) is exceeded. If trap generation is enabled the SEL is only cleared if for one monitor interval no new SEL entry is added or the SEL is completely full (100 %). The default value is disabled. If using this parameter for the 'no' command only the automatic-clearing is disabled but the site remains for monitoring.

Format `set board snmp site` *{local|sel-clear} <ipmb-address>*

Mode Privileged Exec

7.9.26.1 no set board snmp site

This command resets the site used to monitor IPMI information via SNMP.

Format `no set board snmp site` *{local|sel-clear} <ipmb-address>*

Mode Privileged Exec

7.9.27 set board snmp sel-clear

This command specifies the limit in percent for automatic SEL clearing (see 'set board snmp site' above). The default value is 75%.

Format `set board snmp sel-clear limit` *<50..100>*

Mode Privileged Exec

7.9.28 set board snmp interval

This command specified the monitoring interval (for the IPMI information via SNMP) in seconds. The default is 60 seconds.

Format `set boardinfo snmp interval` *<10..6000>*

Mode Privileged Exec

7.9.28.1 no set board snmp interval

This command resets the monitoring interval (for the IPMI information via SNMP) in seconds.

Format `no set boardinfo snmp interval`

Mode Privileged Exec

7.9.29 show boardinfo snmp site

This command displays the site used to monitor IPMI information via SNMP. The site is indicated by ‘local’ for the local site.

Format `show boardinfo snmp interval`

Mode Privileged Exec

7.9.30 show boardinfo snmp interval

This command displays the monitoring interval.

Format `show boardinfo snmp interval`

Mode Privileged Exec

7.9.31 set board snmp trap

This command enables/disables the generation of SNMP traps related to various IPMI information. Following traps can be enabled if the feature is supportedNote, that if “set board snmp trap” is used, the command “set board snmp ipmi-trap” is obsolete (but accepted).

Format
```
set board snmp trap ipmi-sel {enable|disable}
set board snmp trap ipmi-fru {enable|disable}
set board snmp trap health {enable|disable}
```

Mode Privileged Exec

:

<arg>	*Definition*
ipmi-sel	Traps related to IPMI SEL information.
ipmi-fru	Traps related to IPMI FRU information. Traps are sent if a FRU is added, deleted or changed.
health	Traps related to IPMI health information. Traps are sent if the health status has been changed.

7.9.32 show boardinfo snmp trap

This command displays the configured values for generation of SNMP traps. It indicates the state (enable) of various trap generation (see above) as well as all generated filter rules for the IPMI SEL related trap generation.

Note, that if “set board snmp trap” is used, the command “set board snmp ipmi-trap” is obsolete (but accepted).

Format `show boardinfo snmp trap`

Mode Privileged Exec

7.10 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.

7.10.1 authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Default disable

Format **`authorization network radius`**

Mode Global Config

7.10.1.1 no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the radius server.

Format **`no authorization network radius`**

Mode Global Config

7.10.2 radius accounting mode

This command is used to enable the RADIUS accounting function.

Default disabled

Format **`radius accounting mode`**

Mode Global Config

7.10.2.1 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

7.10.3 radius server attribute

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format **`radius server attribute`** *`<4> [<ipaddr>]`*

Mode Global Config

Term	*Definition*
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IP address of the server.

7.10.3.1 no radius server attribute

The `no` version of this command disables the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format **no radius server attribute** *<4> [<ipaddr>]*

Mode Global Config

Example: The following shows an example of the command.

```
(Switch) (Config) #radius server attribute 4  192.168.37.60
(Switch) (Config) #radius server attribute 4
```

7.10.4 radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the 'Default_RADIUS_Auth_Server' and 'Default_RADIUS_Acct_Server' as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the *<auth>* parameter, the command configures the IP address or hostname 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 or hostname 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 or hostname 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 0 - 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|dnsname>} [name <servername>] [port <0-65535>]*

Mode Global Config

Field	*Description*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
0-65535	The port number to use to connect to the specified RADIUS server.
servername	The alias name to identify the server.

7.10.4.1 no radius server host

The no version of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. 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|dnsname>* parameter must match the IP address or dns name of the previously configured RADIUS authentication / accounting server.

Format **no radius server host** *{auth | acct} {<ipaddr|dnsname>}*

Mode Global Config

Example: The following shows an example of the command.

```
(Switch) (Config) #radius server host acct 192.168.37.60
(Switch) (Config) #radius server host acct 192.168.37.60 port 1813
(Switch) (Config) #radius server host auth 192.168.37.60 name
Network1_RADIUS_Auth_Server port 1813

(Switch) (Config) #radius server host acct 192.168.37.60 name
Network2_RADIUS_Auth_Server
(Switch) (Config) #no radius server host acct 192.168.37.60
```

7.10.5 radius server key

This command configures the key to be used in RADIUS client communication with the specified 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 or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports Radius server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Note: The secret must be an alphanumeric value not exceeding 16 characters.

Format **radius server key** *{auth | acct} {<ipaddr|dnsname>}* **encrypted** *<password>*

Mode Global Config

Field	*Description*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
password	The password in encrypted format.

Example: The following shows an example of the CLI command.

```
radius server key acct 10.240.4.10 encrypted <encrypt-string>
```

7.10.6 radius server msgauth

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format **radius server msgauth** *<ipaddr|dnsname>*

Mode Global Config

Field	*Description*
ip addr	The IP address of the server.
dnsname	The DNS name of the server.

7.10.6.1 no radius server msgauth

The `no` version of this command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format **no radius server msgauth** *<ipaddr|dnsname>*

Mode Global Config

7.10.7 radius server primary

This command specifies a configured server that should be the primary server in the group of servers which have the same server name. Multiple primary servers can be configured for each number of servers that have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of specified name, the client uses the primary server that has the specified server name by default. If the RADIUS client fails to communicate with the primary server for any reason, the client uses the backup servers configured with the same server name. These backup servers are identified as the 'Secondary' type.

Format **radius server primary** *{<ipaddr|dnsname>}*

Mode Global Config

Field	*Description*
ip addr	The IP address of the RADIUS Authenticating server.
dnsname	The DNS name of the server.

7.10.8 radius server retransmit

This command configures the global parameter for the RADIUS client that specifies the number of transmissions of the messages to be made before attempting the fall back server upon unsuccessful communication with the current RADIUS authenticating server. When the maximum number of retries are exhausted for the RADIUS accounting server and no response is received, the client does not communicate with any other server.

Default 4

Format **radius server retransmit** *<retries>*

Mode Global Config

Field	Description
retries	The maximum number of transmission attempts in the range of 1 to 15.

7.10.8.1 no radius server retransmit

The no version of this command sets the value of this global parameter to the default value.

Format `no radius server retransmit`
Mode Global Config

7.10.9 radius server timeout

This command configures the global parameter for the RADIUS client that specifies 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

Field	Description
retries	Maximum number of transmission attempts in the range <1-30>.

7.10.9.1 no radius server timeout

The no version of this command sets the timeout global parameter to the default value.

Format `no radius server timeout`
Mode Global Config

7.10.10 show radius

This command displays the values configured for the global parameters of the RADIUS client.

Format `show radius`
Mode Privileged EXEC

Term	Definition
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.

Term	Definition
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request re-transmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

Example: The following shows example CLI display output for the command.

```
(Switch) #show radius

        Number of Configured Authentication Servers..... 32
        Number of Configured Accounting Servers......... 32
        Number of Named Authentication Server Groups.... 15
        Number of Named Accounting Server Groups........ 3
        Number of Retransmits........................... 4
        Time Duration................................... 10
        RADIUS Accounting Mode.......................... Disable
        RADIUS Attribute 4 Mode......................... Enable
        RADIUS Attribute 4 Value ....................... 192.168.37.60
```

7.10.11 show radius servers

This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

Format **show radius servers** *[{ <ipaddr | dnsname> | name [<servername>] }]*

Mode Privileged EXEC

Field	Description
ipaddr	The IP address of the authenticating server.
dnsname	The DNS name of the authenticating server.
servername	The alias name to identify the server.
Current	The '*' symbol preceeding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.

Field	Description
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

Example: The following shows example CLI display output for the command.

```
(Switch) #show radius servers

Cur  Host Address              Server Name                       Port  Type
rent
---- ----------------------- ---------------------------------- ----- ----------
     *   192.168.37.200           Network1_RADIUS_Server           1813  Primary
      192.168.37.201           Network2_RADIUS_Server            1813  Secondary
      192.168.37.202           Network3_RADIUS_Server            1813  Primary
      192.168.37.203           Network4_RADIUS_Server            1813  Secondary

(Switch) #show radius servers name

Current Host Address     Server Name                       Type
-----------------------------------------------------------------192.168.37.200
Network1_RADIUS_Server            Secondary
192.168.37.201           Network2_RADIUS_Server            Primary
192.168.37.202           Network3_RADIUS_Server            Secondary
192.168.37.203           Network4_RADIUS_Server            Primary

(Switch) #show radius servers name Default_RADIUS_Server

Server Name..................................... Default_RADIUS_Server
Host Address.................................... 192.168.37.58
Secret Configured............................... No
Message Authenticator .......................... Enable
Number of Retransmits........................... 4
Time Duration................................... 10
RADIUS Accounting Mode.......................... Disable
RADIUS Attribute 4 Mode......................... Enable
RADIUS Attribute 4 Value ....................... 192.168.37.60

(Switch) #show radius servers 192.168.37.58

Server Name..................................... Default_RADIUS_Server
Host Address.................................... 192.168.37.58
Secret Configured............................... No
Message Authenticator .......................... Enable
Number of Retransmits........................... 4
Time Duration................................... 10
RADIUS Accounting Mode.......................... Disable
RADIUS Attribute 4 Mode......................... Enable
RADIUS Attribute 4 Value ....................... 192.168.37.60
```

7.10.12 show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format **show radius accounting name** *[<servername>]*

Mode Privileged EXEC

Field	*Description*
servername	An alias name to identify the server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Term	*Definition*
Host Address	The IP address of the host.
Server Name	The name of the accounting server.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

Example: The following shows example CLI display output for the command.

```
(Switch) #show radius accounting name

Host Address            Server Name                       Port     Secret
                                                                   Configured
---------------------- --------------------------------- -------- -----------
192.168.37.200          Network1_RADIUS_Server            1813     Yes
192.168.37.201          Network2_RADIUS_Server            1813     No
192.168.37.202          Network3_RADIUS_Server            1813     Yes
192.168.37.203          Network4_RADIUS_Server            1813     No


 (Switch) #show radius accounting name Default_RADIUS_Server

Server Name..................................... Default_RADIUS_Server
Host Address.................................... 192.168.37.200
RADIUS Accounting Mode.......................... Disable
Port ........................................... 1813
Secret Configured .............................. Yes
```

7.10.13 show radius accounting statistics

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format **show radius accounting statistics** *{<ipaddr|dnsname> | name <servername>}*

Mode Privileged EXEC

Term	*Definition*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.

Term	*Definition*
RADIUS Accounting Server Name	The name of the accounting server.
Server Host Address	The IP address of the host.
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 this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this 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 or signature attributes or 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.

Example: The following shows example CLI display output for the command.

```
(Switch) #show radius accounting statistics 192.168.37.200

RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0

(Switch) #show radius accounting statistics name Default_RADIUS_Server

RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
```

```
Unknown Types.............................. 0
Packets Dropped............................ 0
```

7.10.14 show radius statistics

This command displays the summary statistics of configured RADIUS Authenticating servers.

Format **show radius statistics** *{<ipaddr|dnsname> | name <servername>}*

Mode Privileged EXEC

Term	*Definition*
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	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, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that 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 packets of unknown type that 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.

Example: The following shows example CLI display output for the command.

```
(Switch) #show radius statistics 192.168.37.200

RADIUS Server Name.......................... Default_RADIUS_Server
Server Host Address........................ 192.168.37.200
Access Requests............................ 0.00
Access Retransmissions..................... 0
Access Accepts............................. 0
Access Rejects............................. 0
Access Challenges.......................... 0
```

```
Malformed Access Responses..................... 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0

(Switch) #show radius statistics name Default_RADIUS_Server

RADIUS Server Name............................. Default_RADIUS_Server
Server Host Address............................ 192.168.37.200
Access Requests................................ 0.00
Access Retransmissions......................... 0
Access Accepts................................. 0
Access Rejects................................. 0
Access Challenges.............................. 0
Malformed Access Responses..................... 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0
```

7.11 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.

7.11.1 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|hostname>* parameter is the IP address or hostname of the TACACS+ server. To specify multiple hosts, multiple **tacacs-server host** commands can be used.

Format	**tacacs-server host** *<ip-address|hostname>*
Mode	Global Config

7.11.1.1 no tacacs-server host

Use the **no tacacs-server host** command to delete the specified hostname or IP address. The *<ip-address|hostname>* parameter is the IP address of the TACACS+ server.

Format	**no tacacs-server host** *<ip-address|hostname>*
Mode	Global Config

7.11.2 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.

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format **tacacs-server key** [*<key-string>* | *encrypted <key-string>]*

Mode Global Config

7.11.2.1 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

7.11.3 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

7.11.3.1 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

7.11.4 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).

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in

encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format **key** [*<key-string> | encrypted <key-string>]*

Mode TACACS Config

7.11.5 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

7.11.6 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

7.11.7 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

7.11.8 show tacacs

Use the **show tacacs** command to display the configuration and statistics of a TACACS+ server.

Format **show tacacs** *[<ip-address|hostname>]*

Mode Privileged EXEC

Term	*Definition*
IP address or Hostname	The IP address or hostname 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.

7.12 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 6.2.9 “show running-config” on page 6 - 13) to capture the running configuration into a script. Use the **`copy`** command (see 6.4.19 “copy” on page 6 - 25) 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
```

7.12.1 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

7.12.2 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

7.12.3 script list

This command lists all scripts present on the switch as well as the remaining available space.

Format **script list**

Mode Global Config

Term	*Definition*
Configuration Script	Name of the script.
Size	Privileged EXEC

7.12.4 script show

This command displays the contents of a script file, which is named *<scriptname>*.

Format **script show** *<scriptname>*

Mode Privileged EXEC

Term	*Definition*
Output Format	**line** *<number>*: *<line contents>*

7.12.5 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

7.13 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.

7.13.1 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.

Default none

Format **copy** *<tftp://<ipaddr>/<filepath>/<filename>>* **nvram:clibanner**
copy nvram:clibanner *<tftp://<ipaddr>/<filepath>/<filename>>*

Mode Privileged EXEC

7.13.2 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

Appendix A

List of Commands

A. List of Commands

{deny | permit} (IP ACL) ..... 3 - 32
{deny | permit} (IPv6) ..... 3 - 37
{deny | permit} (MAC ACL) ..... 3 - 28
1583compatibility ..... 4 - 36
aaa authentication enable ..... 7 - 19
aaa authentication login ..... 7 - 18
access-list ..... 3 - 31
acl-trapflags ..... 3 - 34
acl-traptimer ..... 3 - 34
addport ..... 2 - 66
advertise speed ..... 2 - 4
area default-cost (OSPF) ..... 4 - 36
area nssa (OSPF) ..... 4 - 36
area nssa default-info-originate (OSPF) ..... 4 - 37
area nssa no-redistribute (OSPF) ..... 4 - 37
area nssa no-summary (OSPF) ..... 4 - 37
area nssa translator-role (OSPF) ..... 4 - 38
area nssa translator-stab-intv (OSPF) ..... 4 - 38
area range (OSPF) ..... 4 - 38
area stub (OSPF) ..... 4 - 39
area stub no-summary (OSPF) ..... 4 - 39
area virtual-link (OSPF) ..... 4 - 39
area virtual-link authentication ..... 4 - 40
area virtual-link dead-interval (OSPF) ..... 4 - 40
area virtual-link hello-interval (OSPF) ..... 4 - 41
area virtual-link retransmit-interval (OSPF) ..... 4 - 41
area virtual-link transmit-delay (OSPF) ..... 4 - 41
arp ..... 4 - 2
arp access-list ..... 2 - 94
arp cachesize ..... 4 - 3
arp dynamicrenew ..... 4 - 3
arp purge ..... 4 - 4
arp resptime ..... 4 - 4
arp retries ..... 4 - 4
arp timeout ..... 4 - 5
assert (filter) ..... 6 - 32
assign-queue ..... 3 - 17
authentication login ..... 2 - 44
authorization network radius ..... 7 - 40
auto-cost (OSPF) ..... 4 - 42
auto-negotiate ..... 2 - 3
auto-negotiate all ..... 2 - 3
auto-summary ..... 4 - 67
auto-voip ..... 3 - 39
auto-voip all ..... 3 - 39

bandwidth ..... 4 - 42
block ..... 2 - 4
boot autoinstall ..... 6 - 62
boot autoinstall auto-save ..... 6 - 62
boot autoinstall retry-count ..... 6 - 62
boot system ..... 6 - 3
bootfile ..... 6 - 42
bootpdhcprelay cidoptmode ..... 4 - 27
bootpdhcprelay maxhopcount ..... 4 - 27
bootpdhcprelay minwaittime ..... 4 - 27
bridge aging-time ..... 2 - 139
cablestatus ..... 6 - 60
capability opaque ..... 4 - 43
class ..... 3 - 18
class-map ..... 3 - 9
class-map rename ..... 3 - 10
classofservice dot1p-mapping ..... 3 - 2
classofservice ip-dscp-mapping ..... 3 - 3
classofservice trust ..... 3 - 3
clear arp-cache ..... 4 - 5
clear arp-switch ..... 4 - 5
clear board event-log ..... 6 - 39
clear config ..... 6 - 21
clear counters ..... 6 - 21
clear dot1x statistics ..... 2 - 45
clear errcounter ..... 6 - 39
clear host ..... 6 - 52
clear igmpsnooping ..... 6 - 21
clear ip arp inspection statistics ..... 2 - 96
clear ip dhcp binding ..... 6 - 46
clear ip dhcp conflict ..... 6 - 47
clear ip dhcp force-client-id ..... 2 - 91
clear ip dhcp server statistics ..... 6 - 46
clear ip helper statistics ..... 4 - 30
clear ip ospf ..... 4 - 43
clear ip ospf configuration ..... 4 - 43
clear ip ospf counters ..... 4 - 43
clear ip ospf neighbor ..... 4 - 43
clear ip ospf neighbor interface ..... 4 - 44
clear ip ospf redistribution ..... 4 - 44
clear isdp counters ..... 2 - 142
clear isdp table ..... 2 - 142
clear lldp remote-data ..... 2 - 120
clear lldp statistics ..... 2 - 120
clear pass ..... 6 - 22
clear port-channel ..... 6 - 22

clear protection-group ..... 3 - 8
clear radius statistics ..... 2 - 45
clear traplog ..... 6 - 22
clear vlan ..... 6 - 22
clicm ..... 7 - 2
client-identifier ..... 6 - 40
client-name ..... 6 - 40
configuration ..... 7 - 6
conform-color ..... 3 - 17
copy ..... 6 - 25
copy (pre-login banner) ..... 7 - 55
copy ipmi-hpm ..... 6 - 27
cos-queue min-bandwidth ..... 3 - 3
cos-queue strict ..... 3 - 4
crypto certificate generate ..... 7 - 11
crypto key generate dsa ..... 7 - 12
crypto key generate rsa ..... 7 - 12
debug arp ..... 6 - 53
debug auto-voip ..... 6 - 53
debug clear ..... 6 - 53
debug console ..... 6 - 54
debug dot1x packet ..... 6 - 54
debug igmpsnooping packet ..... 6 - 54
debug igmpsnooping packet receive ..... 6 - 55
debug igmpsnooping packet transmit ..... 6 - 55
debug isdp packet ..... 2 - 145
debug lacp packet ..... 6 - 56
debug ping packet ..... 6 - 57
debug spanning-tree bpdu ..... 6 - 57
debug spanning-tree bpdu receive ..... 6 - 58
debug spanning-tree bpdu transmit ..... 6 - 58
default-information originate (OSPF) ..... 4 - 44
default-information originate (RIP) ..... 4 - 67
default-metric (OSPF) ..... 4 - 44
default-metric (RIP) ..... 4 - 67
default-router ..... 6 - 40
delete ..... 6 - 2
delete nvram:file <file> ..... 6 - 2
deleteport (Global Config) ..... 2 - 66
deleteport (Interface Config) ..... 2 - 66
description ..... 2 - 4
dhcp client vendor-id-option ..... 2 - 90
dhcp client vendor-id-option-string ..... 2 - 90
dhcp l2relay ..... 2 - 84
dhcp l2relay circuit-id subscription-name ..... 2 - 85
dhcp l2relay circuit-id vlan ..... 2 - 85

dhcp l2relay remote-id subscription-name ..... 2 - 86
dhcp l2relay remote-id vlan ..... 2 - 86
dhcp l2relay subscription-name ..... 2 - 86
dhcp l2relay trust ..... 2 - 87
dhcp l2relay vlan ..... 2 - 87
diffserv ..... 3 - 9
disable (filter) ..... 6 - 31
disconnect ..... 7 - 18
distance ospf (OSPF) ..... 4 - 45
distance rip ..... 4 - 68
distribute-list out (OSPF) ..... 4 - 45
distribute-list out (RIP) ..... 4 - 68
dns-server ..... 6 - 41
domain-name ..... 6 - 43
dos-control all ..... 2 - 131
dos-control firstfrag ..... 2 - 132
dos-control icmp ..... 2 - 133
dos-control icmpfrag ..... 2 - 138
dos-control icmpv4 ..... 2 - 137
dos-control icmpv6 ..... 2 - 138
dos-control l4port ..... 2 - 133
dos-control sipdip ..... 2 - 131
dos-control smacdmac ..... 2 - 134
dos-control tcpfinurgpsh ..... 2 - 137
dos-control tcpflag ..... 2 - 132
dos-control tcpflagseq ..... 2 - 135
dos-control tcpfrag ..... 2 - 132
dos-control tcpoffset ..... 2 - 135
dos-control tcpport ..... 2 - 134
dos-control tcpsyn ..... 2 - 136
dos-control tcpsynfin ..... 2 - 136
dos-control udpport ..... 2 - 135
dot1x default-login ..... 2 - 45
dot1x guest-vlan ..... 2 - 45
dot1x initialize ..... 2 - 45
dot1x login ..... 2 - 46
dot1x max-req ..... 2 - 46
dot1x max-users ..... 2 - 46
dot1x port-control ..... 2 - 46
dot1x port-control all ..... 2 - 47
dot1x re-authenticate ..... 2 - 47
dot1x re-authentication ..... 2 - 48
dot1x system-auth-control ..... 2 - 48
dot1x timeout ..... 2 - 48
dot1x unauthenticated-vlan ..... 2 - 49
dot1x user ..... 2 - 49

drop ..... 3 - 17
dvlan-tunnel ethertype (Global Config) ..... 2 - 30
dvlan-tunnel ethertype default-tpid ..... 2 - 31
enable (filter) ..... 6 - 31
enable (OSPF) ..... 4 - 35
enable (Privileged EXEC access) ..... 7 - 2
enable (RIP) ..... 4 - 66
enable authentication ..... 7 - 20
enable passwd ..... 6 - 22
enable passwd encrypted <password> ..... 6 - 22
enable password ..... 6 - 22
encapsulation ..... 4 - 10
exit-overflow-interval (OSPF) ..... 4 - 45
external-lsdb-limit (OSPF) ..... 4 - 46
hardware-address ..... 6 - 41
host ..... 6 - 41
hostroutesaccept ..... 4 - 69
interface ..... 2 - 3
ip access-group ..... 3 - 33
ip access-list ..... 3 - 32
ip access-list rename ..... 3 - 32
ip address ..... 4 - 7
ip arp inspection filter ..... 2 - 93
ip arp inspection limit ..... 2 - 93
ip arp inspection trust ..... 2 - 93
ip arp inspection validate ..... 2 - 92
ip arp inspection vlan ..... 2 - 92
ip arp inspection vlan logging ..... 2 - 92
ip dhcp bootp automatic ..... 6 - 46
ip dhcp conflict logging ..... 6 - 46
ip dhcp excluded-address ..... 6 - 45
ip dhcp force-client-id ..... 2 - 91
ip dhcp ping packets ..... 6 - 45
ip dhcp pool ..... 6 - 39
ip domain list ..... 6 - 50
ip domain lookup ..... 6 - 49
ip domain name ..... 6 - 49
ip domain retry ..... 6 - 51
ip domain timeout ..... 6 - 51
ip dvmrp ..... 5 - 6
ip dvmrp ..... 5 - 7
ip dvmrp metric ..... 5 - 6
ip dvmrp trapflags ..... 5 - 7
ip helper enable ..... 4 - 33
ip helper-address (Global Config) ..... 4 - 30
ip helper-address (Interface Config) ..... 4 - 31

ip host ..... 6 - 51
ip http authentication ..... 7 - 12
ip http java ..... 7 - 14
ip http secure-port ..... 7 - 17
ip http secure-protocol ..... 7 - 17
ip http secure-server ..... 7 - 14
ip http secure-session hard-timeout ..... 7 - 16
ip http secure-session maxsessions ..... 7 - 16
ip http secure-session soft-timeout ..... 7 - 16
ip http server ..... 7 - 14
ip http session hard-timeout ..... 7 - 15
ip http session maxsessions ..... 7 - 15
ip http session soft-timeout ..... 7 - 15
ip https authentication ..... 7 - 13
ip icmp echo-reply ..... 4 - 73
ip icmp error-interval ..... 4 - 73
ip igmp ..... 5 - 19
ip igmp last-member-query-count ..... 5 - 20
ip igmp last-member-query-interval ..... 5 - 20
ip igmp query-interval ..... 5 - 20
ip igmp query-max-response-time ..... 5 - 21
ip igmp robustness ..... 5 - 21
ip igmp startup-query-count ..... 5 - 21
ip igmp startup-query-interval ..... 5 - 22
ip igmp version ..... 5 - 19
ip igmp-proxy ..... 5 - 25
ip igmp-proxy reset-status ..... 5 - 26
ip igmp-proxy unsolicit-rprt-interval ..... 5 - 25
ip irdp ..... 4 - 16
ip irdp address ..... 4 - 16
ip irdp holdtime ..... 4 - 16
ip irdp maxadvertinterval ..... 4 - 17
ip irdp minadvertinterval ..... 4 - 17
ip irdp preference ..... 4 - 17
ip mcast boundary ..... 5 - 2
ip mtu ..... 4 - 10
ip multicast ..... 5 - 2
ip multicast ttl-threshold ..... 5 - 3
ip name server ..... 6 - 50
ip netdirbcast ..... 4 - 9
ip ospf area ..... 4 - 36
ip ospf authentication ..... 4 - 46
ip ospf cost ..... 4 - 46
ip ospf dead-interval ..... 4 - 47
ip ospf hello-interval ..... 4 - 47
ip ospf mtu-ignore ..... 4 - 49

ip ospf network ..... 4 - 48
ip ospf priority ..... 4 - 48
ip ospf retransmit-interval ..... 4 - 48
ip ospf transmit-delay ..... 4 - 49
ip pimdm (Global Config) ..... 5 - 10
ip pimdm (Interface Config) ..... 5 - 10
ip pimdm hello-interval ..... 5 - 11
ip pimsm ..... 5 - 12
ip pimsm bsr-border ..... 5 - 13
ip pimsm bsr-candidate ..... 5 - 13
ip pimsm dr-priority ..... 5 - 14
ip pimsm hello-interval ..... 5 - 14
ip pimsm join-prune-interval ..... 5 - 14
ip pimsm register-threshold ..... 5 - 15
ip pimsm rp-address ..... 5 - 15
ip pimsm rp-candidate ..... 5 - 15
ip pimsm spt-threshold ..... 5 - 16
ip pimsm ssm ..... 5 - 16
ip pim-trapflags ..... 5 - 16
ip proxy-arp ..... 4 - 3
ip redirects ..... 4 - 72
ip rip ..... 4 - 66
ip rip authentication ..... 4 - 68
ip rip receive version ..... 4 - 69
ip rip send version ..... 4 - 69
ip route ..... 4 - 8
ip route default ..... 4 - 9
ip route distance ..... 4 - 9
ip routing ..... 4 - 7
ip ssh ..... 7 - 9
ip ssh protocol ..... 7 - 10
ip ssh server enable ..... 7 - 10
ip telnet server enable ..... 7 - 7
ip unreachables ..... 4 - 72
ip vrrp (Global Config) ..... 4 - 20
ip vrrp (Interface Config) ..... 4 - 21
ip vrrp authentication ..... 4 - 22
ip vrrp ip ..... 4 - 21
ip vrrp mode ..... 4 - 21
ip vrrp preempt ..... 4 - 22
ip vrrp priority ..... 4 - 22
ip vrrp timers advertise ..... 4 - 23
ip vrrp track interface ..... 4 - 23
ip vrrp track ip route ..... 4 - 24
ipmb (filter) ..... 6 - 31
ipv6 access-list ..... 3 - 36

ipv6 access-list rename ..... 3 - 36
ipv6 traffic-filter ..... 3 - 37
iscsi aging time ..... 3 - 40
iscsi cos ..... 3 - 40
iscsi enable ..... 3 - 41
iscsi target port ..... 3 - 41
isdp advertise-v2 ..... 2 - 142
isdp enabl ..... 2 - 142
isdp holdtime ..... 2 - 141
isdp run ..... 2 - 141
isdp timer ..... 2 - 141
key ..... 7 - 51
L2-port-bridge ..... 2 - 147
lacp actor admin ..... 2 - 67
lacp actor admin key ..... 2 - 67
lacp actor admin state ..... 2 - 68
lacp actor admin state individual ..... 2 - 68
lacp actor admin state longtimeout ..... 2 - 68
lacp actor admin state passive ..... 2 - 69
lacp actor port ..... 2 - 69
lacp actor port priority ..... 2 - 69
lacp actor system priority ..... 2 - 70
lacp admin key ..... 2 - 66
lacp collector max-delay ..... 2 - 67
lacp partner admin key ..... 2 - 70
lacp partner admin state ..... 2 - 71
lacp partner admin state individual ..... 2 - 71
lacp partner admin state longtimeout ..... 2 - 71
lacp partner admin state passive ..... 2 - 72
lacp partner port id ..... 2 - 72
lacp partner port priority ..... 2 - 73
lacp partner system priority ..... 2 - 73
lacp partner system-id ..... 2 - 73
lease ..... 6 - 42
line ..... 7 - 6
lldp med ..... 2 - 124
lldp med all ..... 2 - 125
lldp med confignotification ..... 2 - 125
lldp med confignotification all ..... 2 - 126
lldp med faststartrepeatcount ..... 2 - 126
lldp med transmit-tlv ..... 2 - 125
lldp med transmit-tlv all ..... 2 - 126
lldp notification ..... 2 - 119
lldp notification-interval ..... 2 - 120
lldp receive ..... 2 - 118
lldp timers ..... 2 - 118

lldp transmit ..... 2 - 117
lldp transmit-mgmt ..... 2 - 119
lldp transmit-tlv ..... 2 - 118
logging buffered ..... 6 - 15
logging buffered wrap ..... 6 - 15
logging cli-command ..... 6 - 16
logging console ..... 6 - 16
logging host ..... 6 - 16
logging host remove ..... 6 - 17
logging persistent ..... 6 - 59
logging port ..... 6 - 17
logging syslog ..... 6 - 17
login authentication ..... 7 - 25
logout ..... 6 - 23
mac access-group ..... 3 - 29
mac access-list extended ..... 3 - 27
mac access-list extended rename ..... 3 - 27
macfilter ..... 2 - 81
macfilter adddest ..... 2 - 82
macfilter adddest all ..... 2 - 82
macfilter addsrc ..... 2 - 83
macfilter addsrc all ..... 2 - 83
mark cos ..... 3 - 18
mark cos-as-sec-cos ..... 3 - 19
mark ip-dscp ..... 3 - 19
mark ip-precedence ..... 3 - 19
match any ..... 3 - 10
match class-map ..... 3 - 11
match cos ..... 3 - 11
match destination-address mac ..... 3 - 12
match dstip ..... 3 - 12
match dstip6 ..... 3 - 13
match dstl4port ..... 3 - 13
match ethertype ..... 3 - 10
match ip dscp ..... 3 - 13
match ip precedence ..... 3 - 13
match ip tos ..... 3 - 14
match protocol ..... 3 - 14
match secondary-cos ..... 3 - 12
match secondary-vlan ..... 3 - 16
match source-address mac ..... 3 - 14
match srcip ..... 3 - 15
match srcip6 ..... 3 - 15
match srcl4port ..... 3 - 15
match vlan ..... 3 - 16
maximum-paths (OSPF) ..... 4 - 50

mirror ..... 3 - 17
mode dot1q-tunnel ..... 2 - 31
mode dvlan-tunnel ..... 2 - 32
monitor session ..... 2 - 80
mtu ..... 2 - 5
multicast (interface) ..... 2 - 145
multicast (VLAN) ..... 2 - 146
netbios-name-server ..... 6 - 43
netbios-node-type ..... 6 - 43
network (DHCP Pool Config) ..... 6 - 42
network area (OSPF) ..... 4 - 35
network mac-address ..... 7 - 3
network mac-type ..... 7 - 4
network mgmt_vlan ..... 2 - 21
network parms ..... 7 - 3
network protocol ..... 7 - 3
next-server ..... 6 - 44
no 1583compatibility ..... 4 - 36
no aaa authentication enable ..... 7 - 20
no aaa authentication login ..... 7 - 19
no access-list ..... 3 - 32
no acl-trapflags ..... 3 - 34
no acl-traptimer ..... 3 - 34
no advertise speed ..... 2 - 4
no area nssa default-info-originate (OSPF) ..... 4 - 37
no area nssa no-redistribute (OSPF) ..... 4 - 37
no area nssa no-summary (OSPF) ..... 4 - 38
no area nssa translator-role (OSPF) ..... 4 - 38
no area nssa translator-stab-intv (OSPF) ..... 4 - 38
no area nssa ..... 4 - 37
no area range ..... 4 - 39
no area stub no-summary ..... 4 - 39
no area stub ..... 4 - 39
no area virtual-link authentication ..... 4 - 40
no area virtual-link dead-interval ..... 4 - 40
no area virtual-link hello-interval ..... 4 - 41
no area virtual-link retransmit-interval ..... 4 - 41
no area virtual-link transmit-delay ..... 4 - 42
no area virtual-link ..... 4 - 40
no arp access-list ..... 2 - 94
no arp cachesize ..... 4 - 3
no arp dynamicrenew ..... 4 - 4
no arp resptime ..... 4 - 4
no arp retries ..... 4 - 4
no arp timeout ..... 4 - 5
no arp ..... 4 - 3

no authentication login ..... 2 - 44
no authorization network radius ..... 7 - 40
no auto-cost reference-bandwidth (OSPF) ..... 4 - 42
no auto-negotiate all ..... 2 - 3
no auto-negotiate ..... 2 - 3
no auto-summary ..... 4 - 67
no auto-voip all ..... 3 - 39
no auto-voip ..... 3 - 39
no bandwidth ..... 4 - 42
no block ..... 2 - 4
no boot autoinstall auto-save ..... 6 - 62
no boot autoinstall retry-count ..... 6 - 62
no bootfile ..... 6 - 43
no bootpdhcprelay cidoptmode ..... 4 - 27
no bootpdhcprelay maxhopcount ..... 4 - 27
no bootpdhcprelay minwaittime ..... 4 - 28
no bridge aging-time ..... 2 - 140
no capability opaque ..... 4 - 43
no class ..... 3 - 18
no class-map ..... 3 - 10
no classofservice dot1p-mapping ..... 3 - 2
no classofservice ip-dscp-mapping ..... 3 - 3
no classofservice trust ..... 3 - 3
no client-identifier ..... 6 - 40
no client-name ..... 6 - 40
no cos-queue min-bandwidth ..... 3 - 4
no cos-queue strict ..... 3 - 4
no crypto certificate generate ..... 7 - 12
no crypto key generate dsa ..... 7 - 12
no crypto key generate rsa ..... 7 - 12
no debug arp ..... 6 - 53
no debug auto-voip ..... 6 - 53
no debug console ..... 6 - 54
no debug dot1x packet ..... 6 - 54
no debug igmpsnooping packet ..... 6 - 54
no debug igmpsnooping receive ..... 6 - 56
no debug igmpsnooping transmit ..... 6 - 55
no debug isdp packet ..... 2 - 145
no debug lacp packet ..... 6 - 57
no debug ping packet ..... 6 - 57
no debug spanning-tree bpdu receive ..... 6 - 58
no debug spanning-tree bpdu transmit ..... 6 - 59
no debug spanning-tree bpdu ..... 6 - 58
no default-information originate (OSPF) ..... 4 - 44
no default-information originate (RIP) ..... 4 - 67
no default-metric (OSPF) ..... 4 - 44

no default-metric (RIP) ..... 4 - 67
no default-router ..... 6 - 41
no dhcp client vendor-id-option ..... 2 - 90
no dhcp client vendor-id-option-string ..... 2 - 90
no dhcp l2relay circuit-id subscription-name ..... 2 - 85
no dhcp l2relay circuit-id vlan ..... 2 - 85
no dhcp l2relay remote-id subscription-name ..... 2 - 86
no dhcp l2relay remote-id vlan ..... 2 - 86
no dhcp l2relay subscription-name ..... 2 - 87
no dhcp l2relay trust ..... 2 - 87
no dhcp l2relay vlan ..... 2 - 87
no dhcp l2relay ..... 2 - 85
no diffserv ..... 3 - 9
no distance ospf ..... 4 - 45
no distance rip ..... 4 - 68
no distribute-list out ..... 4 - 45
no distribute-list out ..... 4 - 68
no dns-server ..... 6 - 41
no domain-name ..... 6 - 43
no dos-control all ..... 2 - 131
no dos-control firstfrag ..... 2 - 132
no dos-control icmp ..... 2 - 133
no dos-control icmpfrag ..... 2 - 138
no dos-control icmpv4 ..... 2 - 137
no dos-control icmpv6 ..... 2 - 138
no dos-control l4port ..... 2 - 133
no dos-control sipdip ..... 2 - 132
no dos-control smacdmac ..... 2 - 134
no dos-control tcpfinurgpsh ..... 2 - 137
no dos-control tcpflag ..... 2 - 133
no dos-control tcpflagseq ..... 2 - 135
no dos-control tcpfrag ..... 2 - 132
no dos-control tcpoffset ..... 2 - 136
no dos-control tcpport ..... 2 - 134
no dos-control tcpsyn ..... 2 - 136
no dos-control tcpsynfin ..... 2 - 137
no dos-control udpport ..... 2 - 135
no dot1x guest-vlan ..... 2 - 45
no dot1x max-req ..... 2 - 46
no dot1x max-users ..... 2 - 46
no dot1x port-control all ..... 2 - 47
no dot1x port-control ..... 2 - 47
no dot1x re-authentication ..... 2 - 48
no dot1x system-auth-control ..... 2 - 48
no dot1x timeout ..... 2 - 49
no dot1x unauthenticated-vlan ..... 2 - 49

no dot1x user ..... 2 - 50
no dvlan-tunnel ethertype default–tpid ..... 2 - 31
no enable (OSPF) ..... 4 - 35
no enable (RIP) ..... 4 - 66
no enable authentication ..... 7 - 21
no enable password ..... 6 - 23
no exit-overflow-interval ..... 4 - 46
no external-lsdb-limit ..... 4 - 46
no hardware-address ..... 6 - 41
no host ..... 6 - 42
no hostroutesaccept ..... 4 - 69
no ip access-group ..... 3 - 34
no ip access-list ..... 3 - 32
no ip address ..... 4 - 8
no ip arp inspection filter ..... 2 - 94
no ip arp inspection limit ..... 2 - 93
no ip arp inspection trust ..... 2 - 93
no ip arp inspection validate ..... 2 - 92
no ip arp inspection vlan logging ..... 2 - 92
no ip arp inspection vlan ..... 2 - 92
no ip dhcp bootp automatic ..... 6 - 46
no ip dhcp conflict logging ..... 6 - 46
no ip dhcp excluded-address ..... 6 - 45
no ip dhcp force-client-id ..... 2 - 91
no ip dhcp ping packets ..... 6 - 45
no ip dhcp pool ..... 6 - 40
no ip domain list ..... 6 - 50
no ip domain lookup ..... 6 - 49
no ip domain name ..... 6 - 50
no ip domain retry ..... 6 - 51
no ip domain timeout ..... 6 - 51
no ip dvmrp metric ..... 5 - 6
no ip dvmrp trapflags ..... 5 - 7
no ip dvmrp ..... 5 - 6
no ip dvmrp ..... 5 - 7
no ip helper enable ..... 4 - 33
no ip helper-address (Global Config) ..... 4 - 31
no ip host ..... 6 - 51
no ip http authentication ..... 7 - 13
no ip http java ..... 7 - 14
no ip http secure-port ..... 7 - 17
no ip http secure-server ..... 7 - 14
no ip http secure-session hard-timeout ..... 7 - 16
no ip http secure-session maxsessions ..... 7 - 16
no ip http secure-session soft-timeout ..... 7 - 16
no ip http server ..... 7 - 14

no ip http session hard-timeout....7 - 15
no ip http session maxsessions....7 - 15
no ip http session soft-timeout....7 - 15
no ip https authentication....7 - 13
no ip icmp echo-reply....4 - 73
no ip icmp error-interval....4 - 74
no ip igmp last-member-query-count....5 - 20
no ip igmp last-member-query-interval....5 - 20
no ip igmp query-interval....5 - 20
no ip igmp query-max-response-time....5 - 21
no ip igmp robustness....5 - 21
no ip igmp startup-query-count....5 - 22
no ip igmp startup-query-interval....5 - 22
no ip igmp version....5 - 19
no ip igmp....5 - 19
no ip igmp-proxy unsolicit-rprt-interval....5 - 26
no ip igmp-proxy....5 - 25
no ip irdp address....4 - 16
no ip irdp holdtime....4 - 16
no ip irdp maxadvertinterval....4 - 17
no ip irdp minadvertinterval....4 - 17
no ip irdp preference....4 - 17
no ip irdp....4 - 16
no ip mcast boundary....5 - 2
no ip mtu....4 - 10
no ip multicast ttl-threshold....5 - 3
no ip multicast....5 - 3
no ip name server....6 - 50
no ip netdirbcast....4 - 10
no ip ospf area....4 - 36
no ip ospf authentication....4 - 46
no ip ospf cost....4 - 47
no ip ospf dead-interval....4 - 47
no ip ospf hello-interval....4 - 47
no ip ospf mtu-ignore....4 - 49
no ip ospf network....4 - 48
no ip ospf priority....4 - 48
no ip ospf retransmit-interval....4 - 49
no ip ospf transmit-delay....4 - 49
no ip pimdm (Global Config)....5 - 10
no ip pimdm hello-interval....5 - 11
no ip pimdm mode (Interface Config)....5 - 10
no ip pimsm bsr-border....5 - 13
no ip pimsm bsr-candidate....5 - 13
no ip pimsm dr-priority....5 - 14
no ip pimsm hello-interval....5 - 14

no ip pimsm join-prune-interval ..... 5 - 14
no ip pimsm register-threshold ..... 5 - 15
no ip pimsm rp-address ..... 5 - 15
no ip pimsm rp-candidate ..... 5 - 15
no ip pimsm spt-threshold ..... 5 - 16
no ip pimsm ssm ..... 5 - 16
no ip pimsm ..... 5 - 13
no ip pim-trapflags ..... 5 - 16
no ip proxy-arp ..... 4 - 3
no ip redirects ..... 4 - 73
no ip rip authentication ..... 4 - 68
no ip rip receive version ..... 4 - 69
no ip rip send version ..... 4 - 69
no ip rip ..... 4 - 66
no ip route default ..... 4 - 9
no ip route distance ..... 4 - 9
no ip route ..... 4 - 8
no ip routing ..... 4 - 7
no ip ssh server enable ..... 7 - 10
no ip telnet server enable ..... 7 - 8
no ip unreachables ..... 4 - 72
no ip vrrp authentication ..... 4 - 22
no ip vrrp ip ..... 4 - 22
no ip vrrp mode ..... 4 - 21
no ip vrrp preempt ..... 4 - 22
no ip vrrp priority ..... 4 - 23
no ip vrrp timers advertise ..... 4 - 23
no ip vrrp track interface ..... 4 - 24
no ip vrrp track ip route ..... 4 - 24
no ip vrrp ..... 4 - 21
no ip vrrp ..... 4 - 21
no ipv6 access-list ..... 3 - 36
no ipv6 traffic-filter ..... 3 - 38
no iscsi aging time ..... 3 - 40
no iscsi enable ..... 3 - 41
no isdp advertise-v2 ..... 2 - 142
no isdp enable ..... 2 - 142
no isdp run ..... 2 - 141
no L2-port-bridge ..... 2 - 147
no lacp actor admin key ..... 2 - 67
no lacp actor admin state individual ..... 2 - 68
no lacp actor admin state longtimeout ..... 2 - 69
no lacp actor admin state passive ..... 2 - 69
no lacp actor admin state ..... 2 - 68
no lacp actor port priority ..... 2 - 70
no lacp actor system priority ..... 2 - 70

no lacp admin key ..... 2 - 66
no lacp collector max delay ..... 2 - 67
no lacp partner admin key ..... 2 - 70
no lacp partner admin state individual ..... 2 - 71
no lacp partner admin state longtimeout ..... 2 - 72
no lacp partner admin state passive ..... 2 - 72
no lacp partner admin state ..... 2 - 71
no lacp partner port id ..... 2 - 72
no lacp partner port priority ..... 2 - 73
no lacp partner system priority ..... 2 - 74
no lacp partner system-id ..... 2 - 73
no ldp med confignotification ..... 2 - 125
no lease ..... 6 - 42
no lldp med faststartrepeatcount ..... 2 - 126
no lldp med transmit-tlv ..... 2 - 125
no lldp med transmit-tlv ..... 2 - 126
no lldp med ..... 2 - 124
no lldp notification ..... 2 - 119
no lldp notification-interval ..... 2 - 120
no lldp receive ..... 2 - 118
no lldp timers ..... 2 - 118
no lldp transmit ..... 2 - 118
no lldp transmit-mgmt ..... 2 - 119
no lldp transmit-tlv ..... 2 - 119
no logging buffered wrap ..... 6 - 16
no logging buffered ..... 6 - 15
no logging cli-command ..... 6 - 16
no logging console ..... 6 - 16
no logging persistent ..... 6 - 59
no logging port ..... 6 - 17
no logging syslog ..... 6 - 17
no login authentication ..... 7 - 25
no mac access-group ..... 3 - 29
no mac access-list extended ..... 3 - 27
no macfilter adddest all ..... 2 - 83
no macfilter adddest ..... 2 - 82
no macfilter addsrc all ..... 2 - 83
no macfilter addsrc ..... 2 - 83
no macfilter ..... 2 - 82
no match class-map ..... 3 - 11
no maximum-paths ..... 4 - 50
no mode dot1q-tunnel ..... 2 - 31
no mode dvlan-tunnel ..... 2 - 32
no monitor ..... 2 - 80
no monitor session ..... 2 - 80
no mtu ..... 2 - 5

no netbios-name-server ..... 6 - 43
no netbios-node-type ..... 6 - 44
no network area (OSPF) ..... 4 - 35
no network mac-type ..... 7 - 4
no network mgmt_vlan ..... 2 - 21
no network ..... 6 - 42
no next-server ..... 6 - 44
no option ..... 6 - 44
no passive-interface default ..... 4 - 51
no passive-interface ..... 4 - 51
no password (Line Configuration) ..... 7 - 26
no passwords aging ..... 7 - 27
no passwords history ..... 7 - 27
no passwords lock-out ..... 7 - 27
no passwords min-length ..... 7 - 26
no permit ip host mac host ..... 2 - 94
no policy-map ..... 3 - 20
no port lacpmode all ..... 2 - 75
no port lacpmode ..... 2 - 74
no port lacptimeout ..... 2 - 75
no port lacptimeout ..... 2 - 75
no port-channel adminmode ..... 2 - 76
no port-channel linktrap ..... 2 - 76
no port-channel load-balance ..... 2 - 77
no port-channel static ..... 2 - 74
no port-channel system priority ..... 2 - 78
no port-channel ..... 2 - 65
no port-security mac-address ..... 2 - 116
no port-security max-dynamic ..... 2 - 115
no port-security max-static ..... 2 - 116
no port-security ..... 2 - 115
no protection-group (configure) ..... 3 - 7
no protection-group (interface) ..... 3 - 7
no protocol group ..... 2 - 26
no protocol vlan group all ..... 2 - 27
no protocol vlan group ..... 2 - 26
no radius accounting mode ..... 7 - 40
no radius server attribute ..... 7 - 40
no radius server host ..... 7 - 42
no radius server msgauth ..... 7 - 43
no radius server retransmit ..... 7 - 44
no radius server timeout ..... 7 - 44
no redistribute ..... 4 - 50
no redistribute ..... 4 - 70
no routing ..... 4 - 7
no serial baudrate ..... 7 - 6

no serial timeout ..... 7 - 7
no service dhcp ..... 6 - 45
no service-policy ..... 3 - 21
no set board snmp filter ..... 6 - 31
no set board snmp interval ..... 7 - 38
no set board snmp site ..... 7 - 38
no set bootstopkey ..... 6 - 27
no set chkconfig ..... 6 - 33
no set garp timer join ..... 2 - 39
no set garp timer leave ..... 2 - 39
no set garp timer leaveall ..... 2 - 40
no set gmrp adminmode ..... 2 - 42
no set gmrp interfacemode ..... 2 - 43
no set groupmembership-interval ..... 2 - 108
no set gvrp adminmode ..... 2 - 41
no set gvrp interfacemode ..... 2 - 41
no set igmp fast-leave ..... 2 - 99
no set igmp groupmembership-interval ..... 2 - 99
no set igmp interfacemode ..... 2 - 98
no set igmp maxresponse ..... 2 - 100
no set igmp mcrtrexpiretime ..... 2 - 100
no set igmp mrouter interface ..... 2 - 101
no set igmp mrouter ..... 2 - 101
no set igmp proxy-report interfacemode ..... 2 - 146
no set igmp querier election participate ..... 2 - 105
no set igmp querier query-interval ..... 2 - 104
no set igmp querier timer expiry ..... 2 - 105
no set igmp querier version ..... 2 - 105
no set igmp querier ..... 2 - 104
no set igmp ..... 2 - 98
no set mld fast-leave ..... 2 - 108
no set mld interfacemode ..... 2 - 107
no set mld maxresponse ..... 2 - 109
no set mld mcrtexpiretime ..... 2 - 109
no set mld mrouter interface ..... 2 - 110
no set mld mrouter ..... 2 - 110
no set mld querier election participate ..... 2 - 113
no set mld querier query_interval ..... 2 - 113
no set mld querier timer expiry ..... 2 - 113
no set mld querier ..... 2 - 112
no set mld ..... 2 - 107
no sflow poller ..... 6 - 61
no sflow receiver ..... 6 - 60
no sflow sampler ..... 6 - 61
no shutdown all ..... 2 - 6
no shutdown ..... 2 - 5

no snmp trap link-status all ..... 7 - 34
no snmp trap link-status ..... 7 - 34
no snmp-server community ipaddr ..... 7 - 29
no snmp-server community ipmask ..... 7 - 29
no snmp-server community mode ..... 7 - 30
no snmp-server community ..... 7 - 29
no snmp-server enable traps all ..... 7 - 31
no snmp-server enable traps linkmode ..... 7 - 32
no snmp-server enable traps multiusers ..... 7 - 32
no snmp-server enable traps stpmode ..... 7 - 32
no snmp-server enable traps violation ..... 7 - 31
no snmp-server enable traps ..... 7 - 31
no snmptrap mode ..... 7 - 34
no snmptrap ..... 7 - 33
no snmptrap ..... 7 - 37
no sntp broadcast client poll-interval ..... 6 - 35
no sntp client mode ..... 6 - 35
no sntp client port ..... 6 - 35
no sntp multicast client poll-interval ..... 6 - 37
no sntp server ..... 6 - 37
no sntp unicast client poll-interval ..... 6 - 36
no sntp unicast client poll-retry ..... 6 - 36
no sntp unicast client poll-timeout ..... 6 - 36
no spanning-tree bpdufilter default ..... 2 - 8
no spanning-tree bpdufilter ..... 2 - 8
no spanning-tree bpduflood ..... 2 - 9
no spanning-tree bpduguard ..... 2 - 9
no spanning-tree configuration name ..... 2 - 10
no spanning-tree configuration revision ..... 2 - 10
no spanning-tree edgeport ..... 2 - 10
no spanning-tree forceversion ..... 2 - 11
no spanning-tree forward-time ..... 2 - 11
no spanning-tree guard ..... 2 - 11
no spanning-tree max-age ..... 2 - 12
no spanning-tree max-hops ..... 2 - 12
no spanning-tree mst instance ..... 2 - 13
no spanning-tree mst priority ..... 2 - 14
no spanning-tree mst vlan ..... 2 - 14
no spanning-tree mst ..... 2 - 13
no spanning-tree port mode all ..... 2 - 15
no spanning-tree port mode ..... 2 - 15
no spanning-tree ..... 2 - 8
no split-horizon ..... 4 - 70
no sshcon maxsessions ..... 7 - 10
no sshcon timeout ..... 7 - 11
no storm-control broadcast all level ..... 2 - 57

no storm-control broadcast all rate ..... 2 - 58
no storm-control broadcast all rate ..... 2 - 60
no storm-control broadcast all ..... 2 - 57
no storm-control broadcast level ..... 2 - 56
no storm-control broadcast rate ..... 2 - 56
no storm-control broadcast ..... 2 - 56
no storm-control flowcontrol (AM4904 only) ..... 2 - 63
no storm-control flowcontrol (AM4910 only) ..... 2 - 63
no storm-control multicast all level ..... 2 - 59
no storm-control multicast all ..... 2 - 59
no storm-control multicast level ..... 2 - 58
no storm-control multicast rate ..... 2 - 59
no storm-control multicast ..... 2 - 58
no storm-control unicast all level ..... 2 - 62
no storm-control unicast all rate ..... 2 - 62
no storm-control unicast all ..... 2 - 61
no storm-control unicast level ..... 2 - 61
no storm-control unicast rate ..... 2 - 61
no storm-control unicast ..... 2 - 60
no switchport protected (Global Config) ..... 2 - 37
no switchport protected (Interface Config) ..... 2 - 38
no tacacs-server host ..... 7 - 50
no tacacs-server key ..... 7 - 51
no tacacs-server timeout ..... 7 - 51
no telnetcon maxsessions ..... 7 - 8
no telnetcon timeout ..... 7 - 9
no terminal length ..... 6 - 15
no traffic-shape ..... 3 - 4
no trapflags ..... 4 - 52
no username snmpv3 accessmode ..... 7 - 22
no username snmpv3 authentication ..... 7 - 22
no username snmpv3 encryption ..... 7 - 23
no username ..... 7 - 21
no vlan acceptframe ..... 2 - 22
no vlan association mac ..... 2 - 28
no vlan association subnet ..... 2 - 28
no vlan ingressfilter ..... 2 - 22
no vlan name ..... 2 - 22
no vlan port acceptframe all ..... 2 - 24
no vlan port ingressfilter all ..... 2 - 24
no vlan port pvid all ..... 2 - 24
no vlan port tagging all ..... 2 - 25
no vlan protocol group add protocol ..... 2 - 25
no vlan pvid ..... 2 - 27
no vlan routing ..... 4 - 18
no vlan tagging ..... 2 - 27

no vlan ..... 2 - 21
no voice vlan (Global Config) ..... 2 - 34
no voice vlan (Interface Config) ..... 2 - 34
option ..... 6 - 44
passive-interface (OSPF) ..... 4 - 51
passive-interface default (OSPF) ..... 4 - 50
passwd ..... 7 - 25
password (Line Configuration) ..... 7 - 25
password (User EXEC) ..... 7 - 26
passwords aging ..... 7 - 27
passwords history ..... 7 - 26
passwords lock-out ..... 7 - 27
passwords min-length ..... 7 - 26
permit ip host mac host ..... 2 - 94
ping ..... 6 - 23
police-simple ..... 3 - 19
policy-map ..... 3 - 20
policy-map rename ..... 3 - 20
port ..... 7 - 52
port lacpmode ..... 2 - 74
port lacpmode all ..... 2 - 74
port lacptimeout (Global Config) ..... 2 - 75
port lacptimeout (Interface Config) ..... 2 - 75
port-channel ..... 2 - 65
port-channel adminmode ..... 2 - 75
port-channel hash multicast ..... 2 - 77
port-channel linktrap ..... 2 - 76
port-channel load-balance ..... 2 - 76
port-channel name ..... 2 - 77
port-channel static ..... 2 - 74
port-channel system priority ..... 2 - 77
port-security ..... 2 - 115
port-security mac-address ..... 2 - 116
port-security mac-address move ..... 2 - 116
port-security max-dynamic ..... 2 - 115
port-security max-static ..... 2 - 115
priority ..... 7 - 52
protection-group (configure) ..... 3 - 7
protection-group (interface) ..... 3 - 7
protocol group ..... 2 - 26
protocol vlan group ..... 2 - 26
protocol vlan group all ..... 2 - 26
quit ..... 6 - 24
radius accounting mode ..... 7 - 40
radius server attribute ..... 7 - 40
radius server host ..... 7 - 41

radius server key ..... 7 - 42
radius server msgauth ..... 7 - 43
radius server primary ..... 7 - 43
radius server retransmit ..... 7 - 43
radius server timeout ..... 7 - 44
redirect ..... 3 - 17
redistribute (OSPF) ..... 4 - 50
redistribute (RIP) ..... 4 - 70
reload ..... 6 - 25
reload fast ..... 6 - 25
router ospf ..... 4 - 35
router rip ..... 4 - 66
router-id (OSPF) ..... 4 - 49
routing ..... 4 - 7
script apply ..... 7 - 53
script delete ..... 7 - 54
script list ..... 7 - 54
script show ..... 7 - 54
script validate ..... 7 - 54
serial baudrate ..... 7 - 6
serial timeout ..... 7 - 7
service dhcp ..... 6 - 45
service-policy ..... 3 - 21
serviceport ip ..... 7 - 3
serviceport protocol ..... 7 - 3
set board root-password ..... 6 - 30
set board sensor threshold ..... 6 - 25
set board snmp filter ..... 6 - 31
set board snmp interval ..... 7 - 38
set board snmp ipmi-trap ..... 6 - 31
set board snmp sel-clear ..... 7 - 38
set board snmp site ..... 7 - 38
set board snmp trap ..... 7 - 39
set board time ..... 6 - 30
set bootstopkey ..... 6 - 27
set chkconfig ..... 6 - 32
set garp timer join ..... 2 - 39
set garp timer leave ..... 2 - 39
set garp timer leaveall ..... 2 - 40
set gmrp adminmode ..... 2 - 42
set gmrp interfacemode ..... 2 - 42
set gvrp adminmode ..... 2 - 40
set gvrp interfacemode ..... 2 - 41
set igmp ..... 2 - 97
set igmp fast-leave ..... 2 - 98
set igmp groupmembership-interval ..... 2 - 99

set igmp interfacemode ..... 2 - 98
set igmp maxresponse ..... 2 - 100
set igmp mcrtrexpiretime ..... 2 - 100
set igmp mrouter ..... 2 - 101
set igmp mrouter interface ..... 2 - 101
set igmp proxy-report interfacemode ..... 2 - 146
set igmp querier ..... 2 - 104
set igmp querier election participate ..... 2 - 105
set igmp querier query-interval ..... 2 - 104
set igmp querier timer expiry ..... 2 - 105
set igmp querier version ..... 2 - 105
set mld ..... 2 - 107
set mld fast-leave ..... 2 - 108
set mld groupmembership-interval ..... 2 - 108
set mld interfacemode ..... 2 - 107
set mld maxresponse ..... 2 - 109
set mld mcrtexpiretime ..... 2 - 109
set mld mrouter ..... 2 - 109
set mld mrouter interface ..... 2 - 110
set mld querier ..... 2 - 112
set mld querier election participate ..... 2 - 113
set mld querier query_interval ..... 2 - 112
set mld querier timer expiry ..... 2 - 113
set prompt ..... 7 - 55
set watchdog ..... 6 - 28
sflow poller ..... 6 - 61
sflow receiver ..... 6 - 60
sflow sampler ..... 6 - 60
sfp mode (AM4910 only) ..... 6 - 34
show access-lists ..... 3 - 35
show acl-traptimer ..... 3 - 34
show advertise speed ..... 2 - 4
show arp ..... 4 - 5
show arp access-list ..... 2 - 97
show arp brief ..... 4 - 6
show arp switch ..... 4 - 6
show arp switch ..... 6 - 3
show authentication ..... 2 - 50
show authentication methods ..... 2 - 50
show authentication users ..... 2 - 51
show autoinstall ..... 6 - 62
show auto-voip ..... 3 - 39
show boardinfo address ..... 6 - 29
show boardinfo cpu-load ..... 6 - 30
show boardinfo event-log ..... 6 - 28
show boardinfo fru ..... 6 - 29

show boardinfo ipmidev ..... 6 - 30
show boardinfo memory-usage ..... 6 - 30
show boardinfo post-status ..... 6 - 28
show boardinfo sensors ..... 6 - 28
show boardinfo snmp interval ..... 7 - 39
show boardinfo snmp ipmi-trap ..... 6 - 32
show boardinfo snmp site ..... 7 - 39
show boardinfo snmp trap ..... 7 - 39
show boardinfo time ..... 6 - 30
show boardinfo update-status ..... 6 - 28
show boardinfo version ..... 6 - 29
show bootpdhcprelay ..... 4 - 28
show bootvar ..... 6 - 3
show chkconfig ..... 6 - 33
show class-map ..... 3 - 22
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 dhcp client vendor-id-option ..... 2 - 90
show dhcp l2relay agent-option vlan ..... 2 - 89
show dhcp l2relay all ..... 2 - 88
show dhcp l2relay interface ..... 2 - 88
show dhcp l2relay stats interface ..... 2 - 88
show dhcp l2relay subscription interface ..... 2 - 89
show diffserv ..... 3 - 22
show diffserv service ..... 3 - 25
show diffserv service brief ..... 3 - 25
show dos-control ..... 2 - 138
show dot1q-tunnel ..... 2 - 32
show dot1x ..... 2 - 51
show dot1x clients ..... 2 - 54
show dot1x users ..... 2 - 55
show dvlan-tunnel ..... 2 - 33
show eventlog ..... 6 - 3
show forwardingdb agetime ..... 2 - 140
show garp ..... 2 - 40
show gmrp configuration ..... 2 - 43
show gvrp configuration ..... 2 - 41
show hardware ..... 6 - 4
show hosts ..... 6 - 52
show igmpsnooping ..... 2 - 101
show igmpsnooping mrouter interface ..... 2 - 102
show igmpsnooping mrouter vlan ..... 2 - 103
show igmpsnooping proxy-report ..... 2 - 103
show igmpsnooping querier ..... 2 - 106

show interface ..... 6 - 5
show interface ethernet ..... 6 - 5
show interfaces cos-queue ..... 3 - 6
show interfaces switchport ..... 2 - 38
show ip access-lists ..... 3 - 35
show ip arp inspection ..... 2 - 94
show ip arp inspection interfaces ..... 2 - 96
show ip arp inspection statistics ..... 2 - 95
show ip brief ..... 4 - 11
show ip dhcp binding ..... 6 - 47
show ip dhcp conflict ..... 6 - 49
show ip dhcp force-client-id ..... 2 - 91
show ip dhcp global configuration ..... 6 - 47
show ip dhcp pool configuration ..... 6 - 47
show ip dhcp server statistics ..... 6 - 48
show ip dvmrp ..... 5 - 7
show ip dvmrp interface ..... 5 - 8
show ip dvmrp neighbor ..... 5 - 8
show ip dvmrp nexthop ..... 5 - 9
show ip dvmrp prune ..... 5 - 9
show ip dvmrp route ..... 5 - 9
show ip helper statistics ..... 4 - 34
show ip helper-address ..... 4 - 33
show ip http ..... 7 - 17
show ip igmp ..... 5 - 22
show ip igmp groups ..... 5 - 22
show ip igmp interface ..... 5 - 23
show ip igmp interface membership ..... 5 - 24
show ip igmp interface stats ..... 5 - 25
show ip igmp-proxy ..... 5 - 26
show ip igmp-proxy groups ..... 5 - 27
show ip igmp-proxy groups detail ..... 5 - 28
show ip igmp-proxy interface ..... 5 - 27
show ip interface ..... 4 - 11
show ip interface brief ..... 4 - 12
show ip irdp ..... 4 - 18
show ip mcast ..... 5 - 3
show ip mcast boundary ..... 5 - 4
show ip mcast interface ..... 5 - 4
show ip mcast mroute ..... 5 - 4
show ip mcast mroute group ..... 5 - 5
show ip mcast mroute source ..... 5 - 5
show ip ospf ..... 4 - 53
show ip ospf area ..... 4 - 56
show ip ospf asbr ..... 4 - 57
show ip ospf database ..... 4 - 57

show ip ospf database database-summary ..... 4 - 58
show ip ospf interface ..... 4 - 59
show ip ospf interface brief ..... 4 - 60
show ip ospf interface stats ..... 4 - 61
show ip ospf neighbor ..... 4 - 62
show ip ospf range ..... 4 - 64
show ip ospf statistics ..... 4 - 64
show ip ospf stub table ..... 4 - 65
show ip ospf virtual-link ..... 4 - 65
show ip ospf virtual-link brief ..... 4 - 65
show ip pimdm ..... 5 - 11
show ip pimdm interface ..... 5 - 11
show ip pimdm interface stats ..... 5 - 12
show ip pimdm neighbor ..... 5 - 12
show ip pimsm ..... 5 - 17
show ip pimsm bsr ..... 5 - 17
show ip pimsm interface ..... 5 - 17
show ip pimsm neighbor ..... 5 - 18
show ip pimsm rp mapping ..... 5 - 19
show ip pimsm rphash ..... 5 - 18
show ip rip ..... 4 - 70
show ip rip interface ..... 4 - 71
show ip rip interface brief ..... 4 - 71
show ip route ..... 4 - 13
show ip route preferences ..... 4 - 15
show ip route summary ..... 4 - 14
show ip ssh ..... 7 - 11
show ip stats ..... 4 - 15
show ip vlan ..... 4 - 20
show ip vrrp ..... 4 - 25
show ip vrrp interface ..... 4 - 26
show ip vrrp interface brief ..... 4 - 26
show ip vrrp interface stats ..... 4 - 24
show ipv6 access-lists ..... 3 - 38
show iscsi ..... 3 - 42
show iscsi sessions ..... 3 - 43
show isdp ..... 2 - 143
show isdp entry ..... 2 - 143
show isdp interface ..... 2 - 143
show isdp neighbors ..... 2 - 144
show isdp traffic ..... 2 - 145
show lacp actor ..... 2 - 78
show lacp partner ..... 2 - 78
show lldp ..... 2 - 120
show lldp interface ..... 2 - 121
show lldp local-device ..... 2 - 123

show lldp local-device detail ..... 2 - 124
show lldp med ..... 2 - 127
show lldp med interface ..... 2 - 127
show lldp med local-device detail ..... 2 - 128
show lldp med remote-device ..... 2 - 129
show lldp med remote-device detail ..... 2 - 129
show lldp remote-device ..... 2 - 122
show lldp remote-device detail ..... 2 - 122
show lldp statistics ..... 2 - 121
show logging ..... 6 - 18
show logging backtrace ..... 6 - 39
show logging buffered ..... 6 - 18
show logging errcounter ..... 6 - 39
show logging hosts ..... 6 - 18
show logging traplogs ..... 6 - 19
show loginsession ..... 7 - 18
show mac access-lists ..... 3 - 30
show mac-address-table gmrp ..... 2 - 43
show mac-address-table igmpsnooping ..... 2 - 103
show mac-address-table mldsnooping ..... 2 - 111
show mac-address-table multicast ..... 2 - 140
show mac-address-table static ..... 2 - 84
show mac-address-table staticfiltering ..... 2 - 84
show mac-address-table stats ..... 2 - 141
show mac-addr-table ..... 6 - 11
show mldsnooping ..... 2 - 110
show mldsnooping mrouter interface ..... 2 - 111
show mldsnooping mrouter vlan ..... 2 - 111
show mldsnooping querier ..... 2 - 114
show monitor session ..... 2 - 81
show network ..... 7 - 4
show nvram:file ..... 6 - 19
show passwords configuration ..... 7 - 27
show policy-map ..... 3 - 23
show policy-map interface ..... 3 - 26
show port ..... 2 - 6
show port L2-port-bridge ..... 2 - 147
show port multicast ..... 2 - 146
show port protocol ..... 2 - 7
show port-channel ..... 2 - 79
show port-channel brief ..... 2 - 78
show port-channel hash multicast ..... 2 - 79
show port-channel system priority ..... 2 - 79
show port-security ..... 2 - 116
show port-security dynamic ..... 2 - 117
show port-security static ..... 2 - 117

show port-security violation ..... 2 - 117
show process cpu ..... 6 - 12
show protection-group ..... 3 - 6
show radius ..... 7 - 44
show radius accounting ..... 7 - 46
show radius accounting statistics ..... 7 - 47
show radius servers ..... 7 - 45
show radius statistics ..... 7 - 49
show running-config ..... 6 - 13
show serial ..... 7 - 7
show service-policy ..... 3 - 26
show serviceport ..... 7 - 5
show sflow agent ..... 6 - 61
show sflow receivers ..... 6 - 61
show sflow samplers ..... 6 - 61
show sfp (AM4910 only) ..... 6 - 33
show snmpcommunity ..... 7 - 35
show snmp-engine-id ..... 7 - 38
show snmptrap ..... 7 - 35
show sntp ..... 6 - 37
show sntp client ..... 6 - 38
show sntp server ..... 6 - 38
show spanning-tree ..... 2 - 15
show spanning-tree brief ..... 2 - 16
show spanning-tree interface ..... 2 - 17
show spanning-tree mst port detailed ..... 2 - 17
show spanning-tree mst port summary ..... 2 - 19
show spanning-tree mst summary ..... 2 - 19
show spanning-tree summary ..... 2 - 20
show spanning-tree vlan ..... 2 - 20
show storm-control ..... 2 - 64
show storm-control flowcontrol ..... 2 - 65
show switchport protected ..... 2 - 38
show sysinfo ..... 6 - 14
show tacacs ..... 7 - 52
show tech-support ..... 6 - 14
show telnetcon ..... 7 - 9
show terminal length ..... 6 - 15
show trapflags ..... 7 - 36
show users ..... 7 - 23
show users accounts ..... 7 - 24
show users login-history ..... 7 - 24
show users long ..... 7 - 24
show version ..... 6 - 4
show vlan ..... 2 - 28
show vlan association mac ..... 2 - 30

show vlan association subnet ..... 2 - 30
show vlan brief ..... 2 - 29
show vlan multicast ..... 2 - 146
show vlan port ..... 2 - 29
show voice vlan ..... 2 - 34
show watchdog ..... 6 - 27
shutdown ..... 2 - 5
shutdown all ..... 2 - 5
snmp trap link-status ..... 7 - 34
snmp trap link-status all ..... 7 - 34
snmp-server ..... 7 - 28
snmp-server community ..... 7 - 28
snmp-server community ipaddr ..... 7 - 29
snmp-server community ipmask ..... 7 - 29
snmp-server community mode ..... 7 - 30
snmp-server community ro ..... 7 - 30
snmp-server enable traps ..... 7 - 31
snmp-server enable traps all ..... 7 - 31
snmp-server enable traps linkmode ..... 7 - 31
snmp-server enable traps multiusers ..... 7 - 32
snmp-server enable traps stpmode ..... 7 - 32
snmp-server enable traps violation ..... 7 - 30
snmp-server engine-id ..... 7 - 37
snmptrap ..... 7 - 32
snmptrap ..... 7 - 36
snmptrap ipaddr ..... 7 - 33
snmptrap mode ..... 7 - 33
snmptrap notification ..... 7 - 37
snmptrap snmpversion ..... 7 - 33
sntp broadcast client poll-interval ..... 6 - 34
sntp client mode ..... 6 - 35
sntp client port ..... 6 - 35
sntp multicast client poll-interval ..... 6 - 37
sntp server ..... 6 - 37
sntp unicast client poll-interval ..... 6 - 36
sntp unicast client poll-retry ..... 6 - 36
sntp unicast client poll-timeout ..... 6 - 36
spanning-tree ..... 2 - 7
spanning-tree bpdufilter ..... 2 - 8
spanning-tree bpdufilter default ..... 2 - 8
spanning-tree bpduflood ..... 2 - 8
spanning-tree bpduguard ..... 2 - 9
spanning-tree bpdumigrationcheck ..... 2 - 9
spanning-tree configuration name ..... 2 - 9
spanning-tree configuration revision ..... 2 - 10
spanning-tree edgeport ..... 2 - 10

spanning-tree forceversion ..... 2 - 10
spanning-tree forward-time ..... 2 - 11
spanning-tree guard ..... 2 - 11
spanning-tree max-age ..... 2 - 11
spanning-tree max-hops ..... 2 - 12
spanning-tree mst ..... 2 - 12
spanning-tree mst instance ..... 2 - 13
spanning-tree mst priority ..... 2 - 14
spanning-tree mst vlan ..... 2 - 14
spanning-tree port mode ..... 2 - 14
spanning-tree port mode all ..... 2 - 15
spanning-tree port-state ..... 2 - 15
speed ..... 2 - 6
speed all ..... 2 - 6
split-horizon ..... 4 - 70
sshcon maxsessions ..... 7 - 10
sshcon timeout ..... 7 - 10
status (filter) ..... 6 - 32
storm-control broadcast ..... 2 - 55
storm-control broadcast all ..... 2 - 57
storm-control broadcast all level ..... 2 - 57
storm-control broadcast all rate ..... 2 - 57
storm-control broadcast level ..... 2 - 56
storm-control broadcast rate ..... 2 - 56
storm-control flowcontrol (AM4904 only) ..... 2 - 63
storm-control flowcontrol (AM4910 only) ..... 2 - 62
storm-control multicast ..... 2 - 58
storm-control multicast all ..... 2 - 59
storm-control multicast all level ..... 2 - 59
storm-control multicast all rate ..... 2 - 60
storm-control multicast level ..... 2 - 58
storm-control multicast rate ..... 2 - 58
storm-control unicast ..... 2 - 60
storm-control unicast all ..... 2 - 61
storm-control unicast all level ..... 2 - 62
storm-control unicast all rate ..... 2 - 62
storm-control unicast level ..... 2 - 60
storm-control unicast rate ..... 2 - 61
switchport protected (Global Config) ..... 2 - 37
switchport protected (Interface Config) ..... 2 - 37
tacacs-server host ..... 7 - 50
tacacs-server key ..... 7 - 51
tacacs-server timeout ..... 7 - 51
telnet ..... 7 - 8
telnetcon maxsessions ..... 7 - 8
telnetcon timeout ..... 7 - 8

terminal length ..... 6 - 14
timeout ..... 7 - 52
timers spf ..... 4 - 51
traceroute ..... 6 - 20
traceroute ipv6 ..... 6 - 21
traffic-shape ..... 3 - 4
trapflags (OSPF) ..... 4 - 51
type (filter) ..... 6 - 32
username ..... 7 - 21
username name nopassword ..... 7 - 21
username snmpv3 accessmode ..... 7 - 22
username snmpv3 authentication ..... 7 - 22
username snmpv3 encryption encrypted ..... 7 - 23
username snmpv3 encryption ..... 7 - 22
users defaultlogin ..... 2 - 50
users login ..... 2 - 50
vlan ..... 2 - 21
vlan acceptframe ..... 2 - 21
vlan association mac ..... 2 - 28
vlan association subnet ..... 2 - 27
vlan database ..... 2 - 21
vlan ingressfilter ..... 2 - 22
vlan makestatic ..... 2 - 22
vlan name ..... 2 - 22
vlan participation ..... 2 - 23
vlan participation all ..... 2 - 23
vlan port acceptframe all ..... 2 - 23
vlan port ingressfilter all ..... 2 - 24
vlan port priority all ..... 2 - 36
vlan port pvid all ..... 2 - 24
vlan port tagging all ..... 2 - 25
vlan priority ..... 2 - 37
vlan protocol group ..... 2 - 25
vlan protocol group add protocol ..... 2 - 25
vlan protocol group remove ..... 2 - 26
vlan pvid ..... 2 - 27
vlan routing ..... 4 - 18
vlan tagging ..... 2 - 27
voice vlan (Global Config) ..... 2 - 33
voice vlan (Interface Config) ..... 2 - 34
voice vlan data priority ..... 2 - 34
write memory ..... 7 - 28

Appendix B

FASTPATH log messages

B. FASTPATH Log Messages

This chapter lists common log messages that are provided by FASTPATH, along with information regarding the cause of each message. There is no specific action that can be taken per message. When there is a problem being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem) will assist Broadcom in determining the root cause of such a problem.

Note: This chapter is not a complete list of all syslog messages.

The Log Messages chapter includes the following sections:

- “Core” on page B - 2
- “Utilities” on page B - 3
- “Management” on page B - 5
- “Switching” on page B - 7
- “QoS” on page B - 12
- “Technologies” on page B - 13
- “O/S Support” on page B - 14

B.1 Core

Table 1: BSP Log Messages

Component	*Message*	*Cause*
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting FastPath application.

Table 2: NIM Log Messages

Component	*Message*	*Cause*
NIM	NIM: L7_ATTACH out of order for intIfNum(x) unit x slot x port x	Interface creation out of order
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	There is no mapping between the USP and Interface number
NIM	NIM: L7_DETACH out of order for intIfNum(x) unit x slot x port x	Interface creation out of order
NIM	NIM: L7_DELETE out of order for intIfNum(x) unit x slot x port x	Interface creation out of order
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU)
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created

Table 2: NIM Log Messages (Continued)

Component	Message	Cause
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase
NIM	NIM: Component(x) failed on event(x) for intIfNum(x)	A component responded with a fail indication for an interface event
NIM	NIM: Timeout event(x), intIfNum(x) remainingMask = “xxxx”	A component did not respond before the NIM timeout occurred

Table 3: System Log Messages

Component	Message	Cause
SYSTEM	Configuration file fastpath.cfg size is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file <file name> version <version num>	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.
SYSTEM	File <filename>: same version (version num) but the sizes (<version size>-><expected version size) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	Migrating config file <filename> from version <version num> to <version num>	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.
SYSTEM	Building Defaults	Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.
SYSTEM	sysapiCfgFileGet failed size = <expected size of file> version = <expected version>	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

B.2 Utilities

Table 4: Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: unit/slot/port	An interface changed link state.

Table 5: DHCP Filtering Log Messages

Component	Message	Cause
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	Unable to create semaphore used for dhcp filtering configuration structure .
DHCP Filtering	Failed to register with nv Store.	Unable to register save and restore functions for configuration save
DHCP Filtering	Failed to register with NIM	Unable to register with NIM for interface callback functions
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Error on trying to save configuration .

Table 6: NVStore Log Messages

Component	Message	Cause
NVStore	Building defaults for file XXX	A component's configuration file does not exist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	Error on call to osapiFsWrite routine on file XXX	Either the file cannot be opened or the OS's file I/O returned an error trying to write to the file.
NVStore	File XXX corrupted from file system. Checksum mismatch.	The calculated checksum of a component's configuration file in the file system did not match the checksum of the file in memory.
NVStore	Migrating config file XXX from version Y to Z	A configuration file version mismatch was detected so a configuration file migration has started.

Table 7: RADIUS Log Messages

Component	Message	Cause
RADIUS	RADIUS: Invalid data length - xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Error while attempting to read data from the RADIUS server.
RADIUS	RADIUS: Accounting-Response failed to validate, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.

Table 7: RADIUS Log Messages (Continued)

Component	Message	Cause
RADIUS	RADIUS: Access-Challenge failed to validate, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Access-Accpet failed to validate, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS Client received a server response from an unconfigured server.

Table 8: TACACS+ Log Messages

Component	Message	Cause
TACACS+	TACACS+: authentication error, no server to contact	TACACS+ request needed, but no servers are configured.
TACACS+	TACACS+: connection failed to server x.x.x.x	TACACS+ request sent to server x.x.x.x but no response was received.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	No key configured for the specified server.
TACACS+	TACACS+: received invalid packet type from server.	Received packet type that is not supported.
TACACS+	TACACS+: invalid major version in received packet.	Major version mismatch.
TACACS+	TACACS+: invalid minor version in received packet.	Minor version mismatch.

Table 9: LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 10: SNTP Log Message

Component	Message	Cause
SNTP	SNTP: system clock synchronized on %s UTC	Indicates that SNTP has successfully synchronized the time of the box with the server.

B.3 Management

Table 11: SNMP Log Message

Component	Message	Cause
SNMP	EDB Callback: Unit Join: x.	A new unit has joined the stack.

Table 12: EmWeb Log Messages

Component	Message	Cause
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	A user attempted to connect via telnet when the maximum number of telnet sessions were already active.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	Handle table overflow	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	*ConnectionType* EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.	Socket receive failure.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending : EWOULDBLOCK error sending data	Socket error on send.
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	EmWeb handle index not valid.
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	The receive buffer limit has been reached. Bad request or DoS attack.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

Table 13: CLI_UTIL Log Messages

Component	Message	Cause
CLI_UTIL	Telnet Send Failed errno = 0x%x	Failed to send text string to the telnet client.
CLI_UTIL	osapiFsDir failed	Failed to obtain the directory information from a volume's directory.

Table 14: SSHD Log Messages

Component	Message	Cause
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent
SSHD	SSHD: Unknown UI event in message, event=XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it's an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue

Table 15: SSLT Log Messages

Component	Message	Cause
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.
SSLT	SSLT: Error creating Secure server socket6	Failed to create secure server socket for IPV6.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.
SSLT	SSLT: Msg Queue is full, event=XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event=XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSLcertificate from specified file. XXXX indicates the file from where the certificate is being read.
SSLT	SSLT: Error loading private key from file	Failed while loading private key for SSL connection.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Failed while setting cipher list.
SSLT	SSLT: Could not delete the SSL semaphores	Failed to delete SSL semaphores during cleanup.of all resources associated with the OpenSSL Locking semaphores.

Table 16: User_Manager Log Messages

Component	Message	Cause
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX indicates the username to be authenticated.
User_Manager	Access level for user XXXX could not be determined. Setting to READ_ONLY.	Invalid access level specified for the user. The access level is set to READ_ONLY. XXXX indicates the username.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Failed to migrate the config file. XXXX is the config file name. YYYY is the old version number and ZZZZ is the new version number.

B.4 Switching

Table 17: Protected Ports Log Messages

Component	Message	Cause
Protected Ports	Protected Port: failed to save configuration	This appears when the protected port configuration cannot be saved
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protectedPort	This appears when protectedPortCfgRWLock Fails
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when nimRegisterIntfChange with VLAN fails

Table 17: Protected Ports Log Messages (Continued)

Component	Message	Cause
Protected Ports	Cannot add intIfNum xxx to group yyy	This appears when an interface could not be added to a particular group.
Protected Ports	unable to set protected port group	This appears when a dtl call fails to add interface mask at the driver level
Protected Ports	Cannot delete intIfNum xxx from group yyy	This appears when a dtl call to delete an interface from a group fails
Protected Ports	Cannot update group YYY after deleting interface XXX	This message appears when an update group for a interface deletion fails
Protected Ports	Received an interface change callback while not ready to receive it	This appears when an interface change call back has come before the protected port component is ready.

Table 18: IP Subnet VLANS Log Messages

Component	Message	Cause
IPsubnet vlans	ERROR vlanIpSubnetSubnetValid :Invalid subnet	This occurs when an invalid pair of subnet and netmask has come from the CLI
IPsubnet vlans	IP Subnet Vlans: failed to save configuration	This message appears when save configuration of subnet vlans failed
IPsubnet vlans	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails
IPsubnet vlans	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications
IPsubnet vlans	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
IPsubnet vlans	vlanIpSubnetDtlVlanCreate: Failed	This appears when a dtl call fails to add an entry into the table
IPsubnet vlans	vlanIpSubnetSubnetDeleteApply: Failed	This appears when a dtl fails to delete an entry from the table
IPsubnet vlans	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	This appears when a dtl fails to add an entry for a vlan add notify event.
IPsubnet vlans	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 19: Mac-based VLANs Log Messages

Component	Message	Cause
Mac based VLANS	MAC VLANs: Failed to save configuration	This message appears when save configuration of Mac vlans failed
Mac based VLANS	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	This appears when a read/write lock creations fails
Mac based VLANS	Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications
Mac based VLANS	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
Mac based VLANS	vlanMacAddApply: Failed to add an entry	This appears when a dtl call fails to add an entry into the table
Mac based VLANS	vlanMacDeleteApply: Unable to delete an Entry	This appears when a dtl fails to delete an entry from the table

Table 19: Mac-based VLANs Log Messages

Component	Message	Cause
Mac based VLANS	vlanMacVlanChangeCallback: Failed to add an entry	This appears when a dtl fails to add an entry for a vlan add notify event.
Mac based VLANS	vlanMacVlanChangeCallback: Failed to delete an entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 20: 802.1x Log Messages

Component	Message	Cause
802.1X	*function*: Failed calling dot1xIssueCmd	802.1X message queue is full
802.1X	*function:* EAP message not received from server	RADIUS server did not send required EAP message
802.1X	*function*: Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers
802.1X	*function*: could not set state to <authorized/ unauthorized>, intf xxx	DTL call failed setting authorization state of the port
802.1X	dot1xApplyConfigData: Unable to <enable/ disable> dot1x in driver	DTL call failed enabling/disabling 802.1X
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex=xxx	Failed sending accounting start to RADIUS server
802.1X	*function*: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server

Table 21: IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	*function*: osapiMessageSend failed	IGMP Snooping message queue is full
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Failed to set global IGMP Snooping mode due to message queue being full
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Failed to set interface IGMP Snooping mode due to message queue being full
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Failed to set interface multicast router mode due to IGMP Snooping message queue being full
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Failed to set VLAN IGM Snooping mode due to message queue being full
IGMP Snooping	Failed to set igmp mrouter mode %d for interface xxx on Vlan yyy	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets

Table 22: GARP/GVRP/GMRP Log Messages

Component	Message	Cause
GARP/GVRP/ GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	The garpQueue is full, logs specifics of the message content like internal interface number, type of message etc.
GARP/GVRP/ GMRP	GarpSendPDU: QUEUE SEND FAILURE	The garpPduQueue is full, logs specific of the GPDU, internal interface number, vlan id, buffer handle etc.
GARP/GVRP/ GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.
GARP/GVRP/ GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Traces the build up of message queue. Helpful in determining the load on GARP.
GARP/GVRP/ GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	Mismatch between the gmd (gmrp database) and MFDB.
GARP/GVRP/ GMRP	gmd_create_entry**:** GMRP failure adding MFDB entry: vlan %d and address %s	MFDB table is full.

Table 23: 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully

Table 24: FDB Log Message

Component	Message	Cause
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Unable to set the age time in the hardware

Table 25: Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 26: IPv6 Provisioning Log Message

Component	Message	Cause
IPV6 Provisioning	ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 27: MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry

Table 28: 802.1Q Log Messages

Component	Message	Cause
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan ids. i.e. 4094 - x
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	If this vlan is a learnt via GVRP then we cannot modify it's member set via management.

Table 29: 802.1S Log Messages

Component	Message	Cause
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers

Table 30: Port Mac Locking Log Message

Component	Message	Cause
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 31: Protocol-based VLANs Log Messages

Component	Message	Cause
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with vlans	Appears when vlanRegisterForChange fails to register pbVlan for vlan changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

B.5 QoS

Table 32: ACL Log Messages

Component	Message	Cause
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	ACL *name*, rule *x*: This rule is not being logged	The ACL configuration has resulted in a requirement for more logging rules than the platform supports. The specified rule is functioning normally except for the logging action.
ACL	aclLogTask: error logging ACL rule trap for correlator *number*	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL *number*: Forced truncation of one or more rules during config migration	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Table 33: CoS Log Message

Component	Message	Cause
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	The COS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 34: DiffServ Log Messages

Component	Message	Cause
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	While attempting to clear the running configuration an error was encountered in removing the current settings. This may lead to an inconsistent state in the system and resetting is advised.
DiffServ	Policy invalid for service intf: "policy *name*, intIfNum *x*, direction *y*	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

B.6 Technologies

Table 35: Broadcom Error Messages

Component	Message	Cause
Broadcom	Invalid USP unit = x, slot = x, port =x	A port was not able to be translated correctly during the receive.
Broadcom	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
Broadcom	Failed installing mirror action - rest of the policy applied successfully	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured
Broadcom	Policy x does not contain rule x	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy . Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy
Broadcom	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x	An issue installing the policy due to a possible duplicate hash
Broadcom	ACL x not found in internal table	Attempting to delete a non-existent ACL
Broadcom	ACL internal table overflow	Attempting to add an ACL to a full table
Broadcom	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it's capabilities
Broadcom	USL: failed to put sync response on queue	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out
Broadcom	USL: failed to sync ipmc table on unit=x	Either the transport failed or the message was dropped
Broadcom	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped
Broadcom	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL
Broadcom	USL: failed to sync stg table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn't exist
Broadcom	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer

Table 35: Broadcom Error Messages (Continued)

Component	Message	Cause
Broadcom	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: failed to sync trunk table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer
Broadcom	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer
Broadcom	USL: failed to sync dvlan data on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: failed to sync policy table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: failed to sync VLAN table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI
Broadcom	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
Broadcom	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
Broadcom	Unable to insert route R/P	Route ‘R’ with prefix ‘P’ could not be inserted in the hardware route table. A retry will be issued.
Broadcom	Unable to Insert host H	Host ‘H’ could not be inserted in hardware host table. A retry will be issued.
Broadcom	USL: failed to sync L3 Intf table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: failed to sync L3 Host table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: failed to sync L3 Route table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: failed to sync initiator table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: failed to sync terminator table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
Broadcom	USL: failed to sync ip-multicast table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued

B.7 O/S Support

Table 36: Linux BSP Log Message

Component	Message	Cause
Linux BSP	rc = 10	Second message logged at bootup, right after “Starting code…”. Always logged.

Table 37: OSAPI Linux Log Messages

Component	Message	Cause
OSAPI Linux	osapiNetLinkNeighDump: could not open socket! - or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX	Couldn’t open a “netlink” socket. Make sure “ARP Daemon support” (CONFIG_ARPD) is enabled in the Linux kernel, if the BROADCOM reference kernel binary is not being used.
OSAPI Linux	ipstkNdpFlush: sending delete failed	Failed when telling the kernel to delete a neighbor table entry (the message is incorrect)
OSAPI Linux	unable to open /proc/net/ipv6/conf/default/hop_limit	IPv6 MIB objects read, but /proc filesystem is not mounted, or running kernel does not have IPV6 support
OSAPI Linux	osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ	Error adding or deleting an IPv4 route (listed in hex as YY), on the interface with Linux name ZZ Error code can be looked up in errno.h.
OSAPI Linux	l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: Failed to Delete Route	Error adding or deleting a default gateway in the kernel’s routing table (the function is really osapiRawMRouteAdd()/Delete())
OSAPI Linux	osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: ioctl on XX failed: addr: 0x%YY	Failed trying to set the IP address (in hex as YY) of the interface with Linux name XX, and the interface does not exist. Sometimes this is a harmless race condition (e.g. we try to set address 0 when DHCPing on the network port (dtl0) at bootup, before it’s created using TAP).
OSAPI Linux	ping: sendto error	Trouble sending an ICMP echo request packet for the UI ‘ping’ command. Maybe there was no route to that network.
OSAPI Linux	Failed to Create Interface	Out of memory at system initialization time.
OSAPI Linux	TAP Unable to open XX	The /dev/tap file is missing, or, if not using the BRPOADCOM reference kernel binary, the kernel is missing “Universal TUN/TAP device driver support” (CONFIG_TUN).
OSAPI Linux	Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX	Trouble reading the /dev/tap device, check the error message XX for details.
OSAPI Linux	Log_Init: log file error - creating new log file	This pertains to the “event log” persistent file in flash. Either it did not exist, or had a bad checksum.
OSAPI Linux	Log_Init: Flash (event) log full; erasing	Event log file has been cleared; happens at boot time.
OSAPI Linux	Log_Init: Corrupt event log; erasing	Event log file had a non-blank entry after a blank entry; therefore, something was messed up.

Table 37: OSAPI Linux Log Messages (Continued)

Component	*Message*	*Cause*
OSAPI Linux	Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve Interface Flags	Trouble adding VRRP IP or MAC address(es) to a Linux network interface.

Appendix C

Getting Help

C. 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
4555 Ambroise-Lafortune	Sudetenstrasse 7
Boisbriand, Québec	87600 Kaufbeuren
J7H 0A4 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