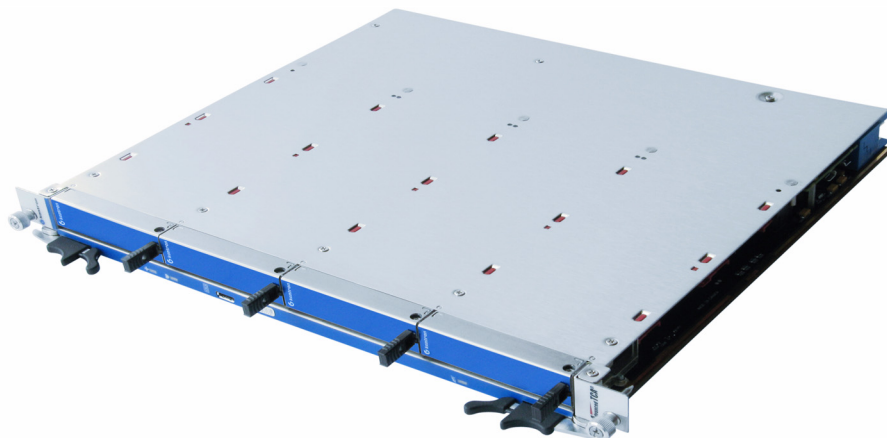


# AT8404 CLI Reference Manual

## AdvancedTCA

M5307\_TECH\_2 Manual ID  
2.06 Revision Index  
19 March, 2010 Date of Issue



---



## Revision History

<b>Publication Title:</b> AT8404 CLI Reference Manual		
<b>ID Number:</b> M5307_Tech_2		
<b>Rev. Index</b>	<b>Brief Description of Changes</b>	<b>Date of Issue</b>
2.00	First Release for AT8404	04 Sept. 2007
2.01	Update commands to FASTPATH 5.0.1.9	19 Dec. 2007
2.02	Update for FASTPATH 5.2, BETA Manual	15 May, 2009
2.03	Final Manual for FASTPATH 5.2	28 July, 2009
2.04	Remove snmp multicast commands, add stratum3 accuracy to set board clock commands, add comment for clear config command	13 Nov, 2009
2.05	Remove download frudata, download fwum commands	23 Nov, 2009
2.06	Editorial changes, remove chapter 4.7 "keying for advanced feaures", fixed errors in chapter 5.16,	19 Mar, 2010

## Imprint

Kontron AG may be contacted via the following:

### North America

Kontron Canada, Inc.  
4555 Ambroise-Lafortune  
Boisbriand, Québec  
J7H 0A4 Canada

Tel: (450) 437-5682  
(800) 354-4223

Fax: (450) 437-8053

E-mail: [support@ca.kontron.com](mailto:support@ca.kontron.com)

### EMEA

Kontron Modular Computers GmbH  
Sudetenstrasse 7  
87600 Kaufbeuren  
Germany

+49 (0) 8341 803 333

+49 (0) 8341 803 339


[support-kom@kontron.com](mailto:support-kom@kontron.com)

For further information about Kontron AG, our products or services, please visit our Internet web site: [www.kontron.com](http://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<sup>®</sup>, the pulse logo, Connecting everything<sup>®</sup>, the Connecting everything logo, and FASTPATH<sup>®</sup> 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 - 2

    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 - 4

    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 - 8

# Chapter 2

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

2.1	Port Configuration Commands .....	2 - 2
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 - 3
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 - 4
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 bpdudfilter .....	2 - 8
2.2.3	spanning-tree bpdudfilter default .....	2 - 8
2.2.4	spanning-tree bpdudflood .....	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 - 9
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 hello-time .....	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 - 13
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	spanning-tree rootguard .....	2 - 15
2.2.23	show spanning-tree .....	2 - 16
2.2.24	show spanning-tree brief .....	2 - 16
2.2.25	show spanning-tree interface .....	2 - 17
2.2.26	show spanning-tree mst port detailed .....	2 - 17
2.2.27	show spanning-tree mst port summary .....	2 - 19
2.2.28	show spanning-tree mst summary .....	2 - 19
2.2.29	show spanning-tree summary .....	2 - 20
2.2.30	show spanning-tree vlan .....	2 - 20





2.3	VLAN Commands	2 - 20
2.3.1	vlan database	2 - 20
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	2 - 30
2.4.2	mode dot1q-tunnel	2 - 31
2.4.3	mode dvlan-tunnel	2 - 31
2.4.4	show dot1q-tunnel	2 - 31
2.4.5	show dvlan-tunnel	2 - 32
2.5	Voice VLAN Commands	2 - 32
2.5.1	voice vlan (Global Config)	2 - 32
2.5.2	voice vlan (Interface Config)	2 - 33
2.5.3	voice vlan data priority	2 - 33
2.5.4	show voice vlan	2 - 33
2.6	Provisioning (IEEE 802.1p) Commands	2 - 34
2.6.1	vlan port priority all	2 - 34
2.6.2	vlan priority	2 - 34
2.7	Protected Ports Commands	2 - 34
2.7.1	switchport protected (Global Config)	2 - 35

2.7.2	switchport protected (Interface Config)	2 - 35
2.7.3	show switchport protected	2 - 36
2.7.4	show interfaces switchport	2 - 36
2.8	GARP Commands	2 - 36
2.8.1	set garp timer join	2 - 36
2.8.2	set garp timer leave	2 - 37
2.8.3	set garp timer leaveall	2 - 37
2.8.4	show garp	2 - 38
2.9	GVRP Commands	2 - 38
2.9.1	set gvrp adminmode	2 - 38
2.9.2	set gvrp interfacemode	2 - 38
2.9.3	show gvrp configuration	2 - 39
2.10	GMRP Commands	2 - 39
2.10.1	set gmrp adminmode	2 - 40
2.10.2	set gmrp interfacemode	2 - 40
2.10.3	show gmrp configuration	2 - 40
2.10.4	show mac-address-table gmrp	2 - 41
2.11	Port-Based Network Access Control Commands	2 - 41
2.11.1	authentication login	2 - 41
2.11.2	clear dot1x statistics	2 - 42
2.11.3	clear radius statistics	2 - 42
2.11.4	dot1x default-login	2 - 42
2.11.5	dot1x guest-vlan	2 - 43
2.11.6	dot1x initialize	2 - 43
2.11.7	dot1x login	2 - 43
2.11.8	dot1x max-req	2 - 43
2.11.9	dot1x max-users	2 - 44
2.11.10	dot1x port-control	2 - 44
2.11.11	dot1x port-control all	2 - 44
2.11.12	dot1x re-authenticate	2 - 45
2.11.13	dot1x re-authentication	2 - 45
2.11.14	dot1x system-auth-control	2 - 45
2.11.15	dot1x timeout	2 - 46
2.11.16	dot1x unauthenticated-vlan	2 - 47
2.11.17	dot1x user	2 - 47
2.11.18	users defaultlogin	2 - 47
2.11.19	users login	2 - 47
2.11.20	show authentication	2 - 48
2.11.21	show authentication users	2 - 48
2.11.22	show dot1x	2 - 48
2.11.23	show dot1x clients	2 - 50
2.11.24	show dot1x users	2 - 51
2.11.25	show users authentication	2 - 51
2.12	Storm-Control Commands	2 - 52
2.12.1	storm-control broadcast	2 - 52

2.12.2	storm-control broadcast level .....	2 - 52
2.12.3	storm-control broadcast rate .....	2 - 53
2.12.4	storm-control broadcast all .....	2 - 53
2.12.5	storm-control broadcast all level .....	2 - 54
2.12.6	storm-control broadcast all rate .....	2 - 54
2.12.7	storm-control multicast .....	2 - 54
2.12.8	storm-control multicast level .....	2 - 55
2.12.9	storm-control multicast rate .....	2 - 55
2.12.10	storm-control multicast all .....	2 - 56
2.12.11	storm-control multicast all level .....	2 - 56
2.12.12	storm-control multicast all rate .....	2 - 56
2.12.13	storm-control unicast .....	2 - 57
2.12.14	storm-control unicast level .....	2 - 57
2.12.15	storm-control unicast rate .....	2 - 58
2.12.16	storm-control unicast all .....	2 - 58
2.12.17	storm-control unicast all level .....	2 - 58
2.12.18	storm-control unicast all rate .....	2 - 59
2.12.19	storm-control flowcontrol .....	2 - 59
2.12.20	show storm-control .....	2 - 60
2.13	Port-Channel/LAG (802.3ad) Commands .....	2 - 61
2.13.1	port-channel .....	2 - 61
2.13.2	addport .....	2 - 61
2.13.3	deleteport (Interface Config) .....	2 - 62
2.13.4	deleteport (Global Config) .....	2 - 62
2.13.5	lACP admin key .....	2 - 62
2.13.6	lACP collector max-delay .....	2 - 62
2.13.7	lACP actor admin .....	2 - 63
2.13.8	lACP actor admin key .....	2 - 63
2.13.9	lACP actor admin state .....	2 - 63
2.13.10	lACP actor admin state individual .....	2 - 64
2.13.11	lACP actor admin state longtimeout .....	2 - 64
2.13.12	lACP actor admin state passive .....	2 - 65
2.13.13	lACP actor port .....	2 - 65
2.13.14	lACP actor port priority .....	2 - 65
2.13.15	lACP actor system priority .....	2 - 65
2.13.16	lACP partner admin key .....	2 - 66
2.13.17	lACP partner admin state .....	2 - 66
2.13.18	lACP partner admin state individual .....	2 - 67
2.13.19	lACP partner admin state longtimeout .....	2 - 67
2.13.20	lACP partner admin state passive .....	2 - 67
2.13.21	lACP partner port id .....	2 - 68
2.13.22	lACP partner port priority .....	2 - 68
2.13.23	lACP partner system-id .....	2 - 69
2.13.24	lACP partner system priority .....	2 - 69
2.13.25	port-channel static .....	2 - 69
2.13.26	port lacpmode .....	2 - 70

2.13.27	port lacpmode all .....	2 - 70
2.13.28	port lacptimeout (Interface Config) .....	2 - 70
2.13.29	port lacptimeout (Global Config) .....	2 - 71
2.13.30	port-channel adminmode .....	2 - 71
2.13.31	port-channel linktrap .....	2 - 72
2.13.32	port-channel load-balance .....	2 - 72
2.13.33	port-channel hash multicast .....	2 - 73
2.13.34	port-channel name .....	2 - 73
2.13.35	port-channel system priority .....	2 - 73
2.13.36	show lacp actor .....	2 - 73
2.13.37	show lacp partner .....	2 - 74
2.13.38	show port-channel brief .....	2 - 74
2.13.39	show port-channel .....	2 - 75
2.13.40	show port-channel system priority .....	2 - 75
2.13.41	show port-channel hash multicast .....	2 - 75
2.14	Port Mirroring .....	2 - 75
2.14.1	monitor session .....	2 - 75
2.14.2	no monitor .....	2 - 76
2.14.3	show monitor session .....	2 - 76
2.15	Static MAC Filtering .....	2 - 77
2.15.1	macfilter .....	2 - 77
2.15.2	macfilter adddest .....	2 - 78
2.15.3	macfilter adddest all .....	2 - 78
2.15.4	macfilter addsrc .....	2 - 78
2.15.5	macfilter addsrc all .....	2 - 79
2.15.6	show mac-address-table static .....	2 - 79
2.15.7	show mac-address-table staticfiltering .....	2 - 80
2.16	DHCP Snooping Configuration Commands .....	2 - 80
2.16.1	ip dhcp snooping .....	2 - 80
2.16.2	ip dhcp snooping vlan .....	2 - 80
2.16.3	ip dhcp snooping verify mac-address .....	2 - 81
2.16.4	ip dhcp snooping database .....	2 - 81
2.16.5	ip dhcp snooping database write-delay .....	2 - 81
2.16.6	ip dhcp snooping binding .....	2 - 82
2.16.7	ip verify binding .....	2 - 82
2.16.8	ip dhcp snooping limit .....	2 - 82
2.16.9	ip dhcp snooping log-invalid .....	2 - 83
2.16.10	ip dhcp snooping trust .....	2 - 83
2.16.11	ip verify source .....	2 - 83
2.16.12	show ip dhcp snooping .....	2 - 84
2.16.13	show ip dhcp snooping binding .....	2 - 84
2.16.14	show ip dhcp snooping database .....	2 - 85
2.16.15	show ip dhcp snooping statistics .....	2 - 85
2.16.16	clear ip dhcp snooping binding .....	2 - 86
2.16.17	clear ip dhcp snooping statistics .....	2 - 86

2.16.18	show ip verify source .....	2 - 86
2.16.19	show ip source binding .....	2 - 87
2.17	Dynamic ARP Inspection Commands .....	2 - 88
2.17.1	ip arp inspection vlan .....	2 - 88
2.17.2	ip arp inspection validate .....	2 - 88
2.17.3	ip arp inspection vlan logging .....	2 - 88
2.17.4	ip arp inspection trust .....	2 - 89
2.17.5	ip arp inspection limit .....	2 - 89
2.17.6	ip arp inspection filter .....	2 - 90
2.17.7	arp access-list .....	2 - 90
2.17.8	permit ip host mac host .....	2 - 90
2.17.9	show ip arp inspection .....	2 - 91
2.17.10	show ip arp inspection statistics .....	2 - 91
2.17.11	clear ip arp inspection statistics .....	2 - 92
2.17.12	show ip arp inspection interfaces .....	2 - 92
2.17.13	show arp access-list .....	2 - 93
2.18	IGMP Snooping Configuration Commands .....	2 - 93
2.18.1	set igmp .....	2 - 93
2.18.2	set igmp interfacemode .....	2 - 94
2.18.3	set igmp fast-leave .....	2 - 95
2.18.4	set igmp groupmembership-interval .....	2 - 95
2.18.5	set igmp maxresponse .....	2 - 96
2.18.6	set igmp mcrtpexpiretime .....	2 - 96
2.18.7	set igmp mrouter .....	2 - 97
2.18.8	set igmp mrouter interface .....	2 - 97
2.18.9	show igmpsnooping .....	2 - 97
2.18.10	show igmpsnooping mrouter interface .....	2 - 98
2.18.11	show igmpsnooping mrouter vlan .....	2 - 99
2.18.12	show mac-address-table igmpsnooping .....	2 - 99
2.19	IGMP Snooping Querier Commands .....	2 - 99
2.19.1	set igmp querier .....	2 - 100
2.19.2	set igmp querier query-interval .....	2 - 100
2.19.3	set igmp querier timer expiry .....	2 - 101
2.19.4	set igmp querier version .....	2 - 101
2.19.5	set igmp querier election participate .....	2 - 101
2.19.6	show igmpsnooping querier .....	2 - 102
2.20	MLD Snooping Commands .....	2 - 102
2.20.1	set mld .....	2 - 103
2.20.2	set mld interfacemode .....	2 - 103
2.20.3	set mld fast-leave .....	2 - 104
2.20.4	set mld groupmembership-interval .....	2 - 104
2.20.5	set mld maxresponse .....	2 - 105
2.20.6	set mld mcrtpexpiretime .....	2 - 105
2.20.7	set mld mrouter .....	2 - 105
2.20.8	set mld mrouter interface .....	2 - 106

2.20.9	show mldsnooping .....	2 - 106
2.20.10	show mldsnooping mrouter interface .....	2 - 107
2.20.11	show mldsnooping mrouter vlan .....	2 - 107
2.20.12	show mac-address-table mldsnooping .....	2 - 107
2.21	MLD Snooping Querier Commands .....	2 - 108
2.21.1	set mld querier .....	2 - 108
2.21.2	set mld querier query_interval .....	2 - 108
2.21.3	set mld querier timer expiry .....	2 - 109
2.21.4	set mld querier election participate .....	2 - 109
2.21.5	show mldsnooping querier .....	2 - 110
2.22	Port Security Commands .....	2 - 111
2.22.1	port-security .....	2 - 111
2.22.2	port-security max-dynamic .....	2 - 111
2.22.3	port-security max-static .....	2 - 111
2.22.4	port-security mac-address .....	2 - 112
2.22.5	port-security mac-address move .....	2 - 112
2.22.6	show port-security .....	2 - 112
2.22.7	show port-security dynamic .....	2 - 113
2.22.8	show port-security static .....	2 - 113
2.22.9	show port-security violation .....	2 - 113
2.23	LLDP (802.1AB) Commands .....	2 - 113
2.23.1	lldp transmit .....	2 - 113
2.23.2	lldp receive .....	2 - 114
2.23.3	lldp timers .....	2 - 114
2.23.4	lldp transmit-tlv .....	2 - 114
2.23.5	lldp transmit-mgmt .....	2 - 115
2.23.6	lldp notification .....	2 - 115
2.23.7	lldp notification-interval .....	2 - 116
2.23.8	clear lldp statistics .....	2 - 116
2.23.9	clear lldp remote-data .....	2 - 116
2.23.10	show lldp .....	2 - 116
2.23.11	show lldp interface .....	2 - 117
2.23.12	show lldp statistics .....	2 - 117
2.23.13	show lldp remote-device .....	2 - 118
2.23.14	show lldp remote-device detail .....	2 - 118
2.23.15	show lldp local-device .....	2 - 119
2.23.16	show lldp local-device detail .....	2 - 120
2.24	LLDP-MED Commands .....	2 - 120
2.24.1	lldp med .....	2 - 120
2.24.2	lldp med confignotification .....	2 - 121
2.24.3	lldp med transmit-tlv .....	2 - 121
2.24.4	lldp med all .....	2 - 122
2.24.5	lldp med confignotification all .....	2 - 122
2.24.6	lldp med faststartrepeatcount .....	2 - 122
2.24.7	lldp med transmit-tlv all .....	2 - 122



2.24.8	show lldp med .....	2 - 123
2.24.9	show lldp med interface .....	2 - 123
2.24.10	show lldp med local-device detail .....	2 - 124
2.24.11	show lldp med remote-device .....	2 - 125
2.24.12	show lldp med remote-device detail .....	2 - 125
2.25	Denial of Service Commands .....	2 - 126
2.25.1	dos-control all .....	2 - 127
2.25.2	dos-control sipdip .....	2 - 127
2.25.3	dos-control firstfrag .....	2 - 127
2.25.4	dos-control tcpfrag .....	2 - 128
2.25.5	dos-control tcpflag .....	2 - 128
2.25.6	dos-control l4port .....	2 - 129
2.25.7	dos-control icmp .....	2 - 129
2.25.8	show dos-control .....	2 - 129
2.26	MAC Database Commands .....	2 - 130
2.26.1	bridge aging-time .....	2 - 130
2.26.2	show forwardingdb agetime .....	2 - 130
2.26.3	show mac-address-table multicast .....	2 - 131
2.26.4	show mac-address-table stats .....	2 - 131
2.27	ISDP Commands .....	2 - 131
2.27.1	isdp run .....	2 - 131
2.27.2	isdp holdtime .....	2 - 132
2.27.3	isdp timer .....	2 - 132
2.27.4	isdp advertise-v2 .....	2 - 132
2.27.5	isdp enable .....	2 - 132
2.27.6	clear isdp counters .....	2 - 133
2.27.7	clear isdp table .....	2 - 133
2.27.8	show isdp .....	2 - 133
2.27.9	show isdp interface .....	2 - 134
2.27.10	show isdp entry .....	2 - 134
2.27.11	show isdp neighbors .....	2 - 134
2.27.12	show isdp traffic .....	2 - 135
2.27.13	debug isdp packet .....	2 - 136
2.28	Multicast Handling Commands .....	2 - 136
2.28.1	multicast (interface) .....	2 - 136
2.28.2	show port multicast .....	2 - 136
2.28.3	multicast (VLAN) .....	2 - 137
2.28.4	show vlan multicast .....	2 - 137
2.28.5	set igmp proxy-report interfacemode .....	2 - 137
2.29	Port Bridging Commands .....	2 - 138
2.29.1	L2-port-bridge .....	2 - 138

# Chapter 3

3.	Quality of Service (QoS) Commands .....	3 - 2
3.1	Class of Service (CoS) Commands .....	3 - 2
3.1.1	classofservice dot1p-mapping .....	3 - 2
3.1.2	classofservice ip-dscp-mapping .....	3 - 3
3.1.3	classofservice trust .....	3 - 3
3.1.4	cos-queue min-bandwidth .....	3 - 3
3.1.5	cos-queue strict .....	3 - 4
3.1.6	traffic-shape .....	3 - 4
3.1.7	show classofservice dot1p-mapping .....	3 - 4
3.1.8	show classofservice ip-precedence-mapping .....	3 - 5
3.1.9	show classofservice ip-dscp-mapping .....	3 - 5
3.1.10	show classofservice trust .....	3 - 5
3.1.11	show interfaces cos-queue .....	3 - 6
3.1.12	show interface cos-counter .....	3 - 6
3.1.13	show packet-memory .....	3 - 6
3.1.14	packet-memory (configure) .....	3 - 7
3.1.15	packet-memory (interface) .....	3 - 7
3.1.16	show protection-group .....	3 - 7
3.1.17	protection-group (configure) .....	3 - 7
3.1.18	protection-group (interface) .....	3 - 8
3.2	Differentiated Services (DiffServ) Commands .....	3 - 8
3.2.1	diffserv .....	3 - 9
3.3	DiffServ Class Commands .....	3 - 9
3.3.1	class-map .....	3 - 10
3.3.2	class-map rename .....	3 - 10
3.3.3	match ethertype .....	3 - 10
3.3.4	match any .....	3 - 11
3.3.5	match class-map .....	3 - 11
3.3.6	match cos .....	3 - 12
3.3.7	match secondary-cos .....	3 - 12
3.3.8	match destination-address mac .....	3 - 12
3.3.9	match dstip .....	3 - 13
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 - 14
3.3.14	match ip tos .....	3 - 14
3.3.15	match protocol .....	3 - 15
3.3.16	match source-address mac .....	3 - 15
3.3.17	match srcip .....	3 - 15



3.3.18	match srcip6 .....	3 - 16
3.3.19	match src4port .....	3 - 16
3.3.20	match vlan .....	3 - 16
3.3.21	match secondary-vlan .....	3 - 16
3.4	DiffServ Policy Commands .....	3 - 17
3.4.1	assign-queue .....	3 - 17
3.4.2	drop .....	3 - 17
3.4.3	mirror .....	3 - 17
3.4.4	redirect .....	3 - 18
3.4.5	conform-color .....	3 - 18
3.4.6	class .....	3 - 18
3.4.7	mark cos .....	3 - 19
3.4.8	mark ip-precedence .....	3 - 19
3.4.9	police-simple .....	3 - 20
3.4.10	policy-map .....	3 - 20
3.4.11	policy-map rename .....	3 - 21
3.5	DiffServ Service Commands .....	3 - 21
3.5.1	service-policy .....	3 - 21
3.6	DiffServ Show Commands .....	3 - 22
3.6.1	show class-map .....	3 - 22
3.6.2	show diffserv .....	3 - 23
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 - 25
3.6.7	show service-policy .....	3 - 26
3.7	MAC Access Control List (ACL) Commands .....	3 - 26
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 - 27
3.7.4	mac access-group .....	3 - 29
3.7.5	show mac access-lists .....	3 - 29
3.8	IP Access Control List (ACL) Commands .....	3 - 30
3.8.1	access-list .....	3 - 30
3.8.2	ip access-list .....	3 - 31
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 - 33
3.8.7	show acl-traptimer .....	3 - 34
3.8.8	acl-traptimer .....	3 - 34
3.8.9	show ip access-lists .....	3 - 34
3.8.10	show access-lists .....	3 - 35
3.9	IPv6 Access Control List (ACL) Commands .....	3 - 35

3.9.1	ipv6 access-list .....	3 - 35
3.9.2	ipv6 access-list rename .....	3 - 36
3.9.3	{deny   permit} (IPv6) .....	3 - 36
3.9.4	ipv6 traffic-filter .....	3 - 37
3.9.5	show ipv6 access-lists .....	3 - 37
3.10	Auto-Voice over IP Commands .....	3 - 38
3.10.1	auto-voip all .....	3 - 38
3.10.2	auto-voip .....	3 - 39
3.10.3	show auto-voip .....	3 - 39

## Chapter 4

4.	Utility Commands .....	4 - 2
4.1	Commands for update and startup Configuration .....	4 - 2
4.1.1	download ipmifw .....	4 - 2
4.1.2	download amcipmifw .....	4 - 2
4.2	Dual Image Commands .....	4 - 3
4.2.1	delete .....	4 - 3
4.2.2	boot system .....	4 - 3
4.2.3	show bootvar .....	4 - 3
4.2.4	filedescr .....	4 - 3
4.3	ATCA commands .....	4 - 3
4.3.1	set board sensor threshold .....	4 - 3
4.3.2	set board device-id .....	4 - 4
4.3.3	show atca ekeying .....	4 - 4
4.3.4	ekeying (interface) .....	4 - 4
4.3.5	ekeying all (configure) .....	4 - 4
4.4	System Information and Statistics Commands .....	4 - 5
4.4.1	show arp switch .....	4 - 5
4.4.2	show eventlog .....	4 - 5
4.4.3	show hardware .....	4 - 6
4.4.4	show version .....	4 - 6
4.4.5	show interface .....	4 - 6
4.4.6	show interface ethernet .....	4 - 7
4.4.7	show mac-addr-table .....	4 - 13
4.4.8	show process cpu .....	4 - 14
4.4.9	show running-config .....	4 - 15
4.4.10	show sysinfo .....	4 - 16
4.4.11	show tech-support .....	4 - 16
4.4.12	terminal length .....	4 - 16
4.4.13	show terminal length .....	4 - 17
4.4.14	show boardinfo post-status .....	4 - 17
4.4.15	show boardinfo sensors .....	4 - 17



4.4.16	show boardinfo event-log .....	4 - 17
4.4.17	show boardinfo update-status .....	4 - 18
4.4.18	show boardinfo version .....	4 - 18
4.4.19	show boardinfo address .....	4 - 18
4.4.20	show boardinfo fru .....	4 - 18
4.4.21	show boardinfo ipmidev .....	4 - 19
4.4.22	show boardinfo amc connection .....	4 - 19
4.4.23	show boardinfo amc fru .....	4 - 19
4.4.24	show boardinfo amc ipmidev .....	4 - 19
4.4.25	show boardinfo led .....	4 - 19
4.4.26	show boardinfo cpu-load .....	4 - 19
4.4.27	show boardinfo memory-usage .....	4 - 20
4.5	Logging Commands .....	4 - 20
4.5.1	logging buffered .....	4 - 20
4.5.2	logging buffered wrap .....	4 - 20
4.5.3	logging cli-command .....	4 - 20
4.5.4	logging console .....	4 - 21
4.5.5	logging host .....	4 - 21
4.5.6	logging host remove .....	4 - 21
4.5.7	logging port .....	4 - 22
4.5.8	logging syslog .....	4 - 22
4.5.9	show logging .....	4 - 22
4.5.10	show logging buffered .....	4 - 23
4.5.11	show logging hosts .....	4 - 23
4.5.12	show logging traplogs .....	4 - 23
4.5.13	clear board event-log .....	4 - 24
4.5.14	show logging backtrace .....	4 - 24
4.5.15	show logging errcounter .....	4 - 24
4.5.16	clear errcounter .....	4 - 24
4.5.17	show logging persistent .....	4 - 24
4.6	System Utility and Clear Commands .....	4 - 25
4.6.1	traceroute .....	4 - 25
4.6.2	clear config .....	4 - 26
4.6.3	clear counters .....	4 - 26
4.6.4	clear igmpsnooping .....	4 - 26
4.6.5	clear pass .....	4 - 26
4.6.6	clear port-channel .....	4 - 27
4.6.7	clear traplog .....	4 - 27
4.6.8	clear vlan .....	4 - 27
4.6.9	enable passwd .....	4 - 27
4.6.10	enable passwd encrypted <password> .....	4 - 27
4.6.11	logout .....	4 - 27
4.6.12	ping .....	4 - 28
4.6.13	quit .....	4 - 29
4.6.14	reload .....	4 - 29
4.6.15	reload fast .....	4 - 29

4.6.16	copy .....	4 - 29
4.6.17	delete nvram:extra-profile .....	4 - 31
4.6.18	set bootstopkey .....	4 - 31
4.7	Simple Network Time Protocol (SNTP) Commands .....	4 - 32
4.7.1	sntp broadcast client poll-interval .....	4 - 32
4.7.2	sntp client mode .....	4 - 32
4.7.3	sntp client port .....	4 - 32
4.7.4	sntp unicast client poll-interval .....	4 - 33
4.7.5	sntp unicast client poll-timeout .....	4 - 33
4.7.6	sntp unicast client poll-retry .....	4 - 33
4.7.7	sntp server .....	4 - 34
4.7.8	show sntp .....	4 - 34
4.7.9	show sntp client .....	4 - 34
4.7.10	show sntp server .....	4 - 35
4.8	DHCP Server Commands .....	4 - 35
4.8.1	ip dhcp pool .....	4 - 35
4.8.2	client-identifier .....	4 - 36
4.8.3	client-name .....	4 - 36
4.8.4	default-router .....	4 - 36
4.8.5	dns-server .....	4 - 37
4.8.6	hardware-address .....	4 - 37
4.8.7	host .....	4 - 37
4.8.8	lease .....	4 - 38
4.8.9	network (DHCP Pool Config) .....	4 - 38
4.8.10	bootfile .....	4 - 38
4.8.11	domain-name .....	4 - 39
4.8.12	netbios-name-server .....	4 - 39
4.8.13	netbios-node-type .....	4 - 39
4.8.14	next-server .....	4 - 40
4.8.15	option .....	4 - 40
4.8.16	ip dhcp excluded-address .....	4 - 41
4.8.17	ip dhcp ping packets .....	4 - 41
4.8.18	service dhcp .....	4 - 41
4.8.19	ip dhcp bootp automatic .....	4 - 42
4.8.20	ip dhcp conflict logging .....	4 - 42
4.8.21	clear ip dhcp binding .....	4 - 42
4.8.22	clear ip dhcp server statistics .....	4 - 42
4.8.23	clear ip dhcp conflict .....	4 - 43
4.8.24	show ip dhcp binding .....	4 - 43
4.8.25	show ip dhcp global configuration .....	4 - 43
4.8.26	show ip dhcp pool configuration .....	4 - 43
4.8.27	show ip dhcp server statistics .....	4 - 44
4.8.28	show ip dhcp conflict .....	4 - 45
4.9	DHCP Filtering .....	4 - 45
4.9.1	ip dhcp filtering .....	4 - 45



4.9.2	ip dhcp filtering trust .....	4 - 46
4.9.3	show ip dhcp filtering .....	4 - 46
4.10	DNS Client Commands .....	4 - 46
4.10.1	ip domain lookup .....	4 - 46
4.10.2	ip domain name .....	4 - 47
4.10.3	ip domain list .....	4 - 47
4.10.4	ip name server .....	4 - 47
4.10.5	ip host .....	4 - 48
4.10.6	ip domain retry .....	4 - 48
4.10.7	ip domain timeout .....	4 - 48
4.10.8	clear host .....	4 - 49
4.10.9	show hosts .....	4 - 49
4.11	Serviceability Packet Tracing Commands .....	4 - 50
4.11.1	debug arp .....	4 - 50
4.11.2	debug auto-voip .....	4 - 50
4.11.3	debug clear .....	4 - 51
4.11.4	debug console .....	4 - 51
4.11.5	debug dot1x packet .....	4 - 51
4.11.6	debug igmpsnooping packet .....	4 - 51
4.11.7	debug igmpsnooping packet transmit .....	4 - 52
4.11.8	debug igmpsnooping packet receive .....	4 - 53
4.11.9	debug ip acl .....	4 - 53
4.11.10	debug ip igmp packet .....	4 - 54
4.11.11	debug ip mcache packet .....	4 - 54
4.11.12	debug lacp packet .....	4 - 54
4.11.13	debug mldsnopping packet .....	4 - 55
4.11.14	debug ping packet .....	4 - 55
4.11.15	debug sflow packet .....	4 - 56
4.11.16	debug spanning-tree bpdu .....	4 - 56
4.11.17	debug spanning-tree bpdu receive .....	4 - 57
4.11.18	debug spanning-tree bpdu transmit .....	4 - 57
4.11.19	logging persistent .....	4 - 58
4.12	Cable Test Command .....	4 - 58
4.12.1	cablestatus .....	4 - 58
4.13	sFlow Commands .....	4 - 59
4.13.1	sflow receiver .....	4 - 59
4.13.2	sflow sampler .....	4 - 60
4.13.3	sflow poller .....	4 - 60
4.13.4	show sflow agent .....	4 - 61
4.13.5	show sflow receivers .....	4 - 62
4.13.6	show sflow samplers .....	4 - 62

# Chapter 5

5.	Management Commands .....	5 - 2
5.1	Network Interface Commands .....	5 - 2
5.1.1	enable (Privileged EXEC access) .....	5 - 2
5.1.2	serviceport ip .....	5 - 2
5.1.3	serviceport protocol .....	5 - 3
5.1.4	network parms .....	5 - 3
5.1.5	network protocol .....	5 - 3
5.1.6	network mac-address .....	5 - 3
5.1.7	network mac-type .....	5 - 4
5.1.8	show network .....	5 - 4
5.1.9	show serviceport .....	5 - 5
5.2	Console Port Access Commands .....	5 - 5
5.2.1	configuration .....	5 - 6
5.2.2	lineconfig .....	5 - 6
5.2.3	serial baudrate .....	5 - 6
5.2.4	serial timeout .....	5 - 6
5.2.5	show serial .....	5 - 7
5.3	Telnet Commands .....	5 - 7
5.3.1	ip telnet server enable .....	5 - 7
5.3.2	telnet .....	5 - 7
5.3.3	transport input telnet .....	5 - 8
5.3.4	transport output telnet .....	5 - 8
5.3.5	session-limit .....	5 - 9
5.3.6	session-timeout .....	5 - 9
5.3.7	telnetcon maxsessions .....	5 - 9
5.3.8	telnetcon timeout .....	5 - 10
5.3.9	show telnet .....	5 - 10
5.3.10	show telnetcon .....	5 - 10
5.4	Secure Shell (SSH) Commands .....	5 - 11
5.4.1	ip ssh .....	5 - 11
5.4.2	ip ssh protocol .....	5 - 11
5.4.3	ip ssh server enable .....	5 - 11
5.4.4	sshcon maxsessions .....	5 - 12
5.4.5	sshcon timeout .....	5 - 12
5.4.6	show ip ssh .....	5 - 12
5.5	Management Security Commands .....	5 - 13
5.5.1	crypto certificate generate .....	5 - 13
5.5.2	crypto key generate rsa .....	5 - 13
5.5.3	crypto key generate dsa .....	5 - 14



5.6	Access Commands .....	5 - 14
5.6.1	disconnect .....	5 - 14
5.6.2	show login session .....	5 - 14
5.7	User Account Commands .....	5 - 15
5.7.1	users name .....	5 - 15
5.7.2	users name <username> unlock .....	5 - 15
5.7.3	users passwd .....	5 - 15
5.7.4	users passwd <username> encrypted <password> .....	5 - 16
5.7.5	users snmpv3 accessmode .....	5 - 16
5.7.6	users snmpv3 authentication .....	5 - 17
5.7.7	users snmpv3 encryption .....	5 - 17
5.7.8	show users .....	5 - 18
5.7.9	show users accounts .....	5 - 18
5.7.10	passwd .....	5 - 18
5.7.11	passwords min-length .....	5 - 19
5.7.12	passwords history .....	5 - 19
5.7.13	passwords aging .....	5 - 19
5.7.14	passwords lock-out .....	5 - 20
5.7.15	show passwords configuration .....	5 - 20
5.7.16	write memory .....	5 - 20
5.8	SNMP Commands .....	5 - 20
5.8.1	snmp-server .....	5 - 21
5.8.2	snmp-server community .....	5 - 21
5.8.3	snmp-server community ipaddr .....	5 - 21
5.8.4	snmp-server community ipmask .....	5 - 22
5.8.5	snmp-server community mode .....	5 - 22
5.8.6	snmp-server community ro .....	5 - 22
5.8.7	snmp-server enable traps violation .....	5 - 23
5.8.8	snmp-server enable traps .....	5 - 23
5.8.9	snmp-server enable traps linkmode .....	5 - 24
5.8.10	snmp-server enable traps multiusers .....	5 - 24
5.8.11	snmp-server enable traps pll .....	5 - 24
5.8.12	snmp-server enable traps stp mode .....	5 - 25
5.8.13	snmptrap .....	5 - 25
5.8.14	snmptrap snmpversion .....	5 - 26
5.8.15	snmptrap ipaddr .....	5 - 26
5.8.16	snmptrap mode .....	5 - 26
5.8.17	snmp trap link-status .....	5 - 26
5.8.18	snmp trap link-status all .....	5 - 27
5.8.19	show snmpcommunity .....	5 - 27
5.8.20	show snmptrap .....	5 - 28
5.8.21	show trapflags .....	5 - 28
5.8.22	snmptrap notification .....	5 - 29
5.8.23	snmp-server engine-id .....	5 - 29
5.8.24	show snmp-engine-id .....	5 - 29
5.8.25	set board snmp site .....	5 - 29

5.8.26	show boardinfo snmp site .....	5 - 30
5.8.27	set board snmp ipmi-trap .....	5 - 30
5.8.28	set board snmp ipmi-trap interval .....	5 - 30
5.8.29	set board snmp ipmi-trap filter .....	5 - 30
5.8.30	enable (filter) .....	5 - 31
5.8.31	disable (filter) .....	5 - 31
5.8.32	ipmb (filter) .....	5 - 31
5.8.33	type (filter) .....	5 - 31
5.8.34	status (filter) .....	5 - 31
5.8.35	assert (filter) .....	5 - 31
5.8.36	show boardinfo snmp ipmi-trap .....	5 - 32
5.9	RADIUS Commands .....	5 - 32
5.9.1	authorization network radius .....	5 - 32
5.9.2	radius accounting mode .....	5 - 32
5.9.3	radius server attribute .....	5 - 32
5.9.4	radius server host .....	5 - 33
5.9.5	radius server key .....	5 - 34
5.9.6	radius server msgauth .....	5 - 35
5.9.7	radius server primary .....	5 - 35
5.9.8	radius server retransmit .....	5 - 36
5.9.9	radius server timeout .....	5 - 36
5.9.10	show radius .....	5 - 36
5.9.11	show radius servers .....	5 - 37
5.9.12	show radius accounting .....	5 - 39
5.9.13	show radius accounting statistics .....	5 - 40
5.9.14	show radius statistics .....	5 - 41
5.10	TACACS+ Commands .....	5 - 42
5.10.1	tacacs-server host .....	5 - 42
5.10.2	tacacs-server key .....	5 - 43
5.10.3	tacacs-server timeout .....	5 - 43
5.10.4	key .....	5 - 44
5.10.5	port .....	5 - 44
5.10.6	priority .....	5 - 44
5.10.7	timeout .....	5 - 44
5.10.8	show tacacs .....	5 - 44
5.11	Configuration Scripting Commands .....	5 - 45
5.11.1	script apply .....	5 - 46
5.11.2	script delete .....	5 - 46
5.11.3	script list .....	5 - 46
5.11.4	script show .....	5 - 46
5.11.5	script validate .....	5 - 46
5.12	Pre-login Banner and System Prompt Commands .....	5 - 47
5.12.1	copy (pre-login banner) .....	5 - 47
5.12.2	set prompt .....	5 - 47
5.13	Diagnostics Commands .....	5 - 47





- 5.13.1 diagnostics ..... 5 - 47
- 5.13.2 show logging diag-report ..... 5 - 47
- 5.14 PCI express Commands ..... 5 - 47
  - 5.14.1 show boardinfo pcie ..... 5 - 47
- 5.15 Storage Commands ..... 5 - 48
  - 5.15.1 set board storage connect ..... 5 - 48
  - 5.15.2 show boardinfo storage ..... 5 - 48
- 5.16 Clock support commands ..... 5 - 48
  - 5.16.1 set board pcie clock ..... 5 - 48
  - 5.16.2 set board pll ..... 5 - 48
  - 5.16.3 show boardinfo pll status ..... 5 - 49
  - 5.16.4 show boardinfo pll config ..... 5 - 49
  - 5.16.5 set board clock bpl ..... 5 - 49
  - 5.16.6 set board clock mux-amc ..... 5 - 49
  - 5.16.7 set board clock mux-bpl ..... 5 - 49
  - 5.16.8 set board clock override ..... 5 - 50
  - 5.16.9 set board clock receiver ..... 5 - 50
  - 5.16.10 set board clock source ..... 5 - 50
  - 5.16.11 show boardinfo clock bpl ..... 5 - 50
  - 5.16.12 show boardinfo clock amc ..... 5 - 51

## Appendix

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

## Appendix

- 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. List of Commands ..... 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 system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

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

- 1.1 “Command Syntax” on page 1 - 2
- 1.2 “Command Conventions” on page 1 - 2
- 1.3 “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 - 4
- 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 - 8

## 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: <b>a (32 bits)</b> <b>a.b (8.24 bits)</b> <b>a.b.c (8.8.16 bits)</b> <b>a.b.c.d (8.8.8.8)</b> In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where <i>n</i> is any valid hexadecimal, octal or decimal number): <b>0xn (CLI assumes hexadecimal format)</b> <b>0n (CLI assumes octal format with leading zeros)</b> <b>n (CLI assumes decimal format)</b>
ipv6-address	<b>FE80:0000:0000:0000:020F:24FF:FEBF:DCB, or</b> <b>FE80:0:0:0:20F:24FF:FEBF:DCB, or</b> <b>FE80::20F24FF:FEBF:DCB, or</b> <b>FE80:0:0:0:20F:24FF:128:141:49:32</b> 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.
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**

<b>Command Mode</b>	<b>Prompt</b>	<b>Mode Description</b>
User EXEC	<code>Switch&gt;</code>	Contains a limited set of commands to view basic system information.
Privileged EXEC	<code>Switch#</code>	Allows you to issue any <b>EXEC</b> command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	<code>Switch (Config)#</code>	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	<code>Switch (Vlan)#</code>	Groups all the VLAN commands.
Interface Config	<code>Switch (Interface &lt;slot/port&gt;)#</code>	Manages the operation of an interface and provides access to the router interface configuration commands.
	<code>Switch (Interface Loopback &lt;id&gt;)#</code>	Use this mode to set up a physical port for a specific logical connection operation.
	<code>Switch (Interface Tunnel &lt;id&gt;)#</code>	
Line Config	<code>Switch (line)#</code>	Contains commands to configure outbound telnet settings and console interface settings.
Policy Map Config	<code>Switch (Config-policy-map)#</code>	Contains the QoS Policy-Map configuration commands.
Policy Class Config	<code>Switch (Config-policy-class-map)#</code>	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	<code>Switch (Config-class-map)#</code>	Contains the QoS class map configuration commands for IPv4.

Table 5: CLI Command Modes (Continued)

Command Mode	Prompt	Mode Description
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 <code>logout</code> .
Privileged EXEC	From the User EXEC mode, enter <code>enable</code> .	To exit to the User EXEC mode, enter <code>exit</code> or press <code>Ctrl-Z</code> .
Global Config	From the Privileged EXEC mode, enter <code>configure</code> .	To exit to the Privileged EXEC mode, enter <code>exit</code> , or press <code>Ctrl-Z</code> .
VLAN Config	From the Privileged EXEC mode, enter <code>vlan database</code> .	To exit to the Privileged EXEC mode, enter <code>exit</code> , or press <code>Ctrl-Z</code> .
Interface Config	From the Global Config mode, enter <code>interface &lt;slot/port&gt;</code> or <code>interface loopback &lt;id&gt;</code> or <code>interface tunnel &lt;id&gt;</code>	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Line Config	From the Global Config mode, enter <code>lineconfig</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Policy-Map Config	From the Global Config mode, enter <code>policy-map</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Policy-Class-Map Config	From the Policy Map mode enter <code>class</code> .	To exit to the Policy Map mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
Class-Map Config	From the Global Config mode, enter <code>class-map</code> , and specify the optional keyword <code>ipv4</code> to specify the Layer 3 protocol for this class. See 3.3.1 “class-map” on page 3 - 10 for more information.	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
MAC Access-list Config	From the Global Config mode, enter <code>mac access-list extended &lt;name&gt;</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
TACACS Config	From the Global Config mode, enter <code>tacacs-server host &lt;ip-addr&gt;</code> , where <code>&lt;ip-addr&gt;</code> is the IP address of the TACACS server on your network.	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .
DHCP Pool Config	From the Global Config mode, enter <code>ip dhcp pool &lt;pool-name&gt;</code> .	To exit to the Global Config mode, enter <code>exit</code> . To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code> .





## 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**

<b>Message Text</b>	<b>Description</b>
% 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**

<b>Key Sequence</b>	<b>Description</b>
DEL or Backspace	Delete previous character
Ctrl-A	Go to beginning of line
Ctrl-E	Go to end of line
Ctrl-F	Go forward one character
Ctrl-B	Go backward one character
Ctrl-D	Delete current character
Ctrl-U, X	Delete to beginning of line
Ctrl-K	Delete to end of line
Ctrl-W	Delete previous word
Ctrl-T	Transpose previous character
Ctrl-P	Go to previous line in history buffer
Ctrl-R	Rewrites or pastes the line
Ctrl-N	Go to next line in history buffer
Ctrl-Y	Prints last deleted character
Ctrl-Q	Enables serial flow



**Table 8: CLI Editing Conventions (Continued)**

<b>Key Sequence</b>	<b>Description</b>
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 5.1 “Network Interface Commands” on page 5 - 2.





---

*Chapter* **2**

---

---

# Switching Commands

---



## 2. Switching Commands

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

The Switching Commands chapter includes the following sections:

- 2.1 “Port Configuration Commands” on page 2 - 2
- 2.2 “Spanning Tree Protocol (STP) Commands” on page 2 - 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 - 32
- 2.6 “Provisioning (IEEE 802.1p) Commands” on page 2 - 34
- 2.7 “Protected Ports Commands” on page 2 - 34
- 2.8 “GARP Commands” on page 2 - 36
- 2.9 “GVRP Commands” on page 2 - 38
- 2.10 “GMRP Commands” on page 2 - 39
- 2.11 “Port-Based Network Access Control Commands” on page 2 - 41
- 2.12 “Storm-Control Commands” on page 2 - 52
- 2.13 “Port-Channel/LAG (802.3ad) Commands” on page 2 - 61
- 2.14 “Port Mirroring” on page 2 - 75
- 2.15 “Static MAC Filtering” on page 2 - 77
- 2.16 “DHCP Snooping Configuration Commands” on page 2 - 80
- 2.17 “Dynamic ARP Inspection Commands” on page 2 - 88
- 2.18 “IGMP Snooping Configuration Commands” on page 2 - 93
- 2.19 “IGMP Snooping Querier Commands” on page 2 - 99
- 2.20 “MLD Snooping Commands” on page 2 - 102
- 2.21 “MLD Snooping Querier Commands” on page 2 - 108
- 2.22 “Port Security Commands” on page 2 - 111
- 2.23 “LLDP (802.1AB) Commands” on page 2 - 113
- 2.24 “LLDP-MED Commands” on page 2 - 120
- 2.25 “Denial of Service Commands” on page 2 - 126
- 2.26 “MAC Database Commands” on page 2 - 130
- 2.27 “ISDP Commands” on page 2 - 131
- 2.28 “Multicast Handling Commands” on page 2 - 136
- 2.29 “Port Bridging Commands” on page 2 - 138



**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>}`

**Mode** Interface Config

Acceptable Values	Definition
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

### 2.1.12 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
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Type</b>	If not blank, this field indicates that this port is a special type of port. The possible values are: <ul style="list-style-type: none"> <li>• <b>Mirror</b> - this port is a monitoring port. For more information, see 2.14 “Port Mirroring” on page 2 - 75.</li> <li>• <b>PC Mbr</b> - this port is a member of a port-channel (LAG).</li> <li>• <b>Probe</b> - this port is a probe port.</li> </ul>
<b>Admin Mode</b>	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.
<b>Physical Mode</b>	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.
<b>Physical Status</b>	The port speed and duplex mode.
<b>Link Status</b>	The Link is up or down.



<b>Term</b>	<b>Definition</b>
<b>Link Trap</b>	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
<b>LACP Mode</b>	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

<b>Term</b>	<b>Definition</b>
<b>Group Name</b>	The group name of an entry in the Protocol-based VLAN table.
<b>Group ID</b>	The group identifier of the protocol group.
<b>Protocol(s)</b>	The type of protocol(s) for this group.
<b>VLAN</b>	The VLAN associated with this Protocol Group.
<b>Interface(s)</b>	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 bpdudfilter

Use this command to enable BPDU Filter on the interface.

<b>Default</b>	disabled
<b>Format</b>	<code>spanning-tree bpdudfilter</code>
<b>Mode</b>	Interface Config

### 2.2.2.1 no spanning-tree bpdudfilter

Use this command to disable BPDU Filter on the interface.

<b>Default</b>	disabled
<b>Format</b>	<code>no spanning-tree bpdudfilter</code>
<b>Mode</b>	Interface Config

## 2.2.3 spanning-tree bpdudfilter default

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

<b>Default</b>	disabled
<b>Format</b>	<code>spanning-tree bpdudfilter</code>
<b>Mode</b>	Global Config

### 2.2.3.1 no spanning-tree bpdudfilter default

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

<b>Default</b>	disabled
<b>Format</b>	<code>no spanning-tree bpdudfilter default</code>
<b>Mode</b>	Global Config

## 2.2.4 spanning-tree bpduflood

Use this command to enable BPDU Flood on the interface.

<b>Default</b>	disabled
<b>Format</b>	<code>spanning-tree bpduflood</code>
<b>Mode</b>	Interface Config

### 2.2.4.1 no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface.

<b>Default</b>	disabled
<b>Format</b>	<code>no spanning-tree bpduflood</code>
<b>Mode</b>	Interface Config



## 2.2.5 spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

<b>Default</b>	disabled
<b>Format</b>	<code>spanning-tree bpduguard</code>
<b>Mode</b>	Global Config

### 2.2.5.1 no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

<b>Default</b>	disabled
<b>Format</b>	<code>no spanning-tree bpduguard</code>
<b>Mode</b>	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.

<b>Format</b>	<code>spanning-tree bpdumigrationcheck {&lt;slot/port&gt;   all}</code>
<b>Mode</b>	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.

<b>Default</b>	base MAC address in hexadecimal notation
<b>Format</b>	<code>spanning-tree configuration name &lt;name&gt;</code>
<b>Mode</b>	Global Config

### 2.2.7.1 no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

<b>Format</b>	<code>no spanning-tree configuration name</code>
<b>Mode</b>	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.

<b>Default</b>	0
<b>Format</b>	<code>spanning-tree configuration revision &lt;0-65535&gt;</code>



**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 hello-time

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

**Default** 2  
**Format** `spanning-tree hello-time <1-10>`  
**Mode** Interface Config

### 2.2.12.1 no spanning-tree hello-time

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

**Format** `no spanning-tree hello-time`  
**Mode** Interface Config

## 2.2.13 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  $2 \times (\text{Bridge Forward Delay} - 1)$ .

**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 <1-127>`  
**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 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

**Default**            none  
**Format**            `spanning-tree mst instance <mstid>`  
**Mode**             Global Config

#### 2.2.16.1 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..4094). 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 spanning-tree rootguard

Use this command to enable root BPDU Guard on the interface.

**Default**            disabled  
**Format**            `spanning-tree rootguard`  
**Mode**             Interface Config

### 2.2.22.1 no spanning-tree rootguard

Use this command to disable root BPDU Guard on the interface.

**Format**            `no spanning-tree rootguard`  
**Mode**             Interface Config



### 2.2.23 show spanning-tree

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

<b>Format</b>	<code>show spanning-tree</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>Privileged EXEC</li> <li>User EXEC</li> </ul>

<i>Term</i>	<i>Definition</i>
<b>Bridge Priority</b>	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.
<b>Bridge Identifier</b>	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
<b>Time Since Topology Change</b>	Time in seconds.
<b>Topology Change Count</b>	Number of times changed.
<b>Topology Change</b>	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.
<b>Designated Root</b>	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
<b>Root Path Cost</b>	Value of the Root Path Cost parameter for the common and internal spanning tree.
<b>Root Port Identifier</b>	Identifier of the port to access the Designated Root for the CST
<b>Root Port Max Age</b>	Derived value.
<b>Root Port Bridge Forward Delay</b>	Derived value
<b>Hello Time</b>	Configured value of the parameter for the CST.
<b>Bridge Hold Time</b>	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
<b>Bridge Max Hops</b>	Bridge max-hops count for the device.
<b>CST Regional Root</b>	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
<b>Regional Root Path Cost</b>	Path Cost to the CST Regional Root.
<b>Associated FIDs</b>	List of forwarding database identifiers currently associated with this instance.
<b>Associated VLANs</b>	List of VLAN IDs currently associated with this instance.

### 2.2.24 show spanning-tree brief

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

<b>Format</b>	<code>show spanning-tree brief</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>Privileged EXEC</li> <li>User EXEC</li> </ul>

<i>Term</i>	<i>Definition</i>
<b>Bridge Priority</b>	Configured value.
<b>Bridge Identifier</b>	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.



<i>Term</i>	<i>Definition</i>
<b>Bridge Max Age</b>	Configured value.
<b>Bridge Max Hops</b>	Bridge max-hops count for the device.
<b>Bridge Hello Time</b>	Configured value.
<b>Bridge Forward Delay</b>	Configured value.
<b>Bridge Hold Time</b>	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

### 2.2.25 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.

<b>Format</b>	<code>show spanning-tree interface &lt;slot/port&gt;</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

<i>Term</i>	<i>Definition</i>
<b>Hello Time</b>	Admin hello time for this port.
<b>Port Mode</b>	Enabled or disabled.
<b>BPDU Filter</b>	Enabled or disabled.
<b>BPDU Flood</b>	Enabled or disabled.
<b>BPDU Guard</b>	Enabled or disabled.
<b>Root Guard</b>	Enabled or disabled.
<b>Port Up Time Since Counters Last Cleared</b>	Time since port was reset, displayed in days, hours, minutes, and seconds.
<b>STP BPDUs Transmitted</b>	Spanning Tree Protocol Bridge Protocol Data Units sent.
<b>STP BPDUs Received</b>	Spanning Tree Protocol Bridge Protocol Data Units received.
<b>RST BPDUs Transmitted</b>	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
<b>RST BPDUs Received</b>	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
<b>MSTP BPDUs Transmitted</b>	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
<b>MSTP BPDUs Received</b>	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

### 2.2.26 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.

<b>Format</b>	<code>show spanning-tree mst port detailed &lt;mstid&gt; &lt;slot/port&gt;</code>
---------------	---



- Mode**
- Privileged EXEC
  - User EXEC

<b>Term</b>	<b>Definition</b>
<b>MST Instance ID</b>	The ID of the existing MST instance.
<b>Port Identifier</b>	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.
<b>Port Priority</b>	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
<b>Port Forwarding State</b>	Current spanning tree state of this port.
<b>Port Role</b>	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
<b>Auto-Calculate Port Path Cost</b>	Indicates whether auto calculation for port path cost is enabled.
<b>Port Path Cost</b>	Configured value of the Internal Port Path Cost parameter.
<b>Auto-Calculate External Port Path Cost</b>	Indicates whether auto calculation for external port path cost is enabled.
<b>External Port Path Cost</b>	Configured value of the external Port Path Cost parameter.
<b>Designated Root</b>	The Identifier of the designated root for this port.
<b>Designated Port Cost</b>	Path Cost offered to the LAN by the Designated Port.
<b>Designated Bridge</b>	Bridge Identifier of the bridge with the Designated Port.
<b>Designated Port Identifier</b>	Port on the Designated Bridge that offers the lowest cost to the LAN.

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

<b>Term</b>	<b>Definition</b>
<b>Port Identifier</b>	The port identifier for this port within the CST.
<b>Port Priority</b>	The priority of the port within the CST.
<b>Port Forwarding State</b>	The forwarding state of the port within the CST.
<b>Port Role</b>	The role of the specified interface within the CST.
<b>Port Path Cost</b>	The configured path cost for the specified interface.
<b>Designated Root</b>	Identifier of the designated root for this port within the CST.
<b>Designated Port Cost</b>	Path Cost offered to the LAN by the Designated Port.
<b>Designated Bridge</b>	The bridge containing the designated port.
<b>Designated Port Identifier</b>	Port on the Designated Bridge that offers the lowest cost to the LAN.
<b>Topology Change Acknowledgement</b>	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
<b>Hello Time</b>	The hello time in use for this port.
<b>Edge Port</b>	The configured value indicating if this port is an edge port.



<i>Term</i>	<i>Definition</i>
<b>Edge Port Status</b>	The derived value of the edge port status. True if operating as an edge port; false otherwise.
<b>Point To Point MAC Status</b>	Derived value indicating if this port is part of a point to point link.
<b>CST Regional Root</b>	The regional root identifier in use for this port.
<b>CST Port Cost</b>	The configured path cost for this port.

## 2.2.27 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

<i>Term</i>	<i>Definition</i>
<b>MST Instance ID</b>	The MST instance associated with this port.
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>STP Mode</b>	Indicates whether spanning tree is enabled or disabled on the port.
<b>Type</b>	Currently not used.
<b>STP State</b>	The forwarding state of the port in the specified spanning tree instance.
<b>Port Role</b>	The role of the specified port within the spanning tree.
<b>Desc</b>	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

## 2.2.28 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

<i>Term</i>	<i>Definition</i>
<b>MST Instance ID List</b>	List of multiple spanning trees IDs currently configured.
<b>For each MSTID:</b>	<ul style="list-style-type: none"> <li>• List of forwarding database identifiers associated with this instance.</li> <li>• Associated FIDs    • List of VLAN IDs associated with this instance.</li> <li>• Associated VLANs</li> </ul>



### 2.2.29 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

<i>Term</i>	<i>Definition</i>
<b>Spanning Tree Adminmode</b>	Enabled or disabled.
<b>Spanning Tree Version</b>	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
<b>BPDU Guard Mode</b>	Enabled or disabled.
<b>BPDU Filter Mode</b>	Enabled or disabled.
<b>Configuration Name</b>	Identifier used to identify the configuration currently being used.
<b>Configuration Revision Level</b>	Identifier used to identify the configuration currently being used.
<b>Configuration Digest Key</b>	Identifier used to identify the configuration currently being used.
<b>MST Instances</b>	List of all multiple spanning tree instances configured on the switch.

### 2.2.30 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

<i>Term</i>	<i>Definition</i>
<b>VLAN Identifier</b>	The VLANs associated with the selected MST instance.
<b>Associated Instance</b>	Identifier for the associated multiple spanning tree instance or “CST” if associated with the common and internal spanning tree.

## 2.3 VLAN Commands

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

### 2.3.1 vlan database

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

**Format**            `vlan database`  
**Mode**             Privileged EXEC





### 2.3.2 network mgmt\_vlan

This command configures the Management VLAN ID.

**Default** 1  
**Format** `network mgmt_vlan <1-4069>`  
**Mode** Privileged EXEC

#### 2.3.2.1 no network mgmt\_vlan

This command sets the Management VLAN ID to the default.

**Format** `no network mgmt_vlan`  
**Mode** Privileged EXEC

### 2.3.3 vlan

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

**Format** `vlan <2-4094>`  
**Mode** VLAN Config

#### 2.3.3.1 no vlan

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

**Format** `no vlan <2-4094>`  
**Mode** VLAN Config

### 2.3.4 vlan acceptframe

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

**Default** all  
**Format** `vlan acceptframe {vlanonly | all}`  
**Mode** Interface Config

#### 2.3.4.1 no vlan acceptframe

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

**Format** `no vlan acceptframe`  
**Mode** Interface Config



### 2.3.5 **vlan ingressfilter**

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

<b>Default</b>	disabled
<b>Format</b>	<code>vlan ingressfilter</code>
<b>Mode</b>	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.

<b>Format</b>	<code>no vlan ingressfilter</code>
<b>Mode</b>	Interface Config

### 2.3.6 **vlan makestatic**

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

<b>Format</b>	<code>vlan makestatic &lt;2-4094&gt;</code>
<b>Mode</b>	VLAN Config

### 2.3.7 **vlan name**

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

<b>Default</b>	<ul style="list-style-type: none"><li>• VLAN ID 1 - default</li><li>• other VLANS - blank string</li></ul>
<b>Format</b>	<code>vlan name &lt;2-4094&gt; &lt;name&gt;</code>
<b>Mode</b>	VLAN Config

#### 2.3.7.1 **no vlan name**

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

<b>Format</b>	<code>no vlan name &lt;2-4094&gt;</code>
<b>Mode</b>	VLAN Config



### 2.3.8 vlan participation

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

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

Participation options are:

<b>Participation Options</b>	<b>Definition</b>
<b>include</b>	The interface is always a member of this VLAN. This is equivalent to registration fixed.
<b>exclude</b>	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
<b>auto</b>	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} <1-4094>`  
**Mode** Global Config

You can use the following participation options:

<b>Participation Options</b>	<b>Definition</b>
<b>include</b>	The interface is always a member of this VLAN. This is equivalent to registration fixed.
<b>exclude</b>	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
<b>auto</b>	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:

<b>Mode</b>	<b>Definition</b>
<b>VLAN Only mode</b>	Untagged frames or priority frames received on this interface are discarded.
<b>Admit All mode</b>	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 <1-4094>

**Mode** Global Config

### 2.3.12.1 no vlan port pvid all

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

**Format** no vlan port pvid all

**Mode** Global Config



### 2.3.13 `vlan port tagging all`

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

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

#### 2.3.13.1 `no vlan port tagging all`

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

**Format** `no vlan port tagging all`  
**Mode** Global Config

### 2.3.14 `vlan protocol group`

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

**Format** `vlan protocol group <groupname>`  
**Mode** Global Config

### 2.3.15 `vlan protocol group add protocol`

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



**Note:** FASTPATH software supports IPv4 protocol-based VLANs.

**Default** none  
**Format** `vlan protocol group add protocol <groupid> <protocol>`  
**Mode** Global Config

#### 2.3.15.1 `no vlan protocol group add protocol`

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

**Format** `no vlan protocol group add protocol <groupid> <protocol>`  
**Mode** Global Config



### 2.3.16 vlan protocol group remove

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

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

**Mode**             Global Config

### 2.3.17 protocol group

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

**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 <1-4094>`  
**Mode**        Interface Config

### 2.3.20.1      no vlan pvid

This command sets the VLAN ID per interface to 1.

**Format**      `no vlan pvid`  
**Mode**        Interface Config

## 2.3.21        vlan tagging

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

**Format**      `vlan tagging <1-4094>`  
**Mode**        Interface Config

### 2.3.21.1      no vlan tagging

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

**Format**      `no vlan tagging <1-4094>`  
**Mode**        Interface Config

## 2.3.22        vlan association subnet

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

**Format**      `vlan association subnet <ipaddr> <netmask> <vlanid>`  
**Mode**        VLAN Config



### 2.3.22.1 no vlan association subnet

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

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

**Mode**             VLAN Config

### 2.3.23 vlan association mac

This command associates a MAC address to a VLAN.

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

**Mode**             VLAN database

### 2.3.23.1 no vlan association mac

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

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

**Mode**             VLAN database

### 2.3.24 show vlan

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

**Format**            `show vlan <vlanid>`

**Mode**             • Privileged EXEC  
• User EXEC

<i>Term</i>	<i>Definition</i>
<b>VLAN ID</b>	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
<b>VLAN Name</b>	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.
<b>VLAN Type</b>	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).
<b>Interface</b>	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.
<b>Current</b>	The degree of participation of this port in this VLAN. The permissible values are: <ul style="list-style-type: none"> <li>• <b>Include</b> - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</li> <li>• <b>Exclude</b> - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</li> <li>• <b>Autodetect</b> - 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.</li> </ul>





<b>Term</b>	<b>Definition</b>
<b>Configured</b>	The configured degree of participation of this port in this VLAN. The permissible values are: <ul style="list-style-type: none"> <li>• <b>Include</b> - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</li> <li>• <b>Exclude</b> - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</li> <li>• <b>Autodetect</b> - 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.</li> </ul>
<b>Tagging</b>	The tagging behavior for this port in this VLAN. <ul style="list-style-type: none"> <li>• <b>Tagged</b> - Transmit traffic for this VLAN as tagged frames.</li> <li>• <b>Untagged</b> - Transmit traffic for this VLAN as untagged frames.</li> </ul>

### 2.3.25 show vlan brief

This command displays a list of all configured VLANs.

<b>Format</b>	<code>show vlan brief</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

<b>Term</b>	<b>Definition</b>
<b>VLAN ID</b>	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4094.
<b>VLAN Name</b>	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.
<b>VLAN Type</b>	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.

<b>Format</b>	<code>show vlan port {&lt;slot/port&gt;   all}</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

<b>Term</b>	<b>Definition</b>
<b>Interface</b>	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.
<b>Port VLAN ID</b>	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.
<b>Acceptable Frame Types</b>	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.



<i>Term</i>	<i>Definition</i>
<b>Ingress Filtering</b>	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.
<b>GVRP</b>	May be enabled or disabled.
<b>Default Priority</b>	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

<i>Term</i>	<i>Definition</i>
<b>IP Address</b>	The IP address assigned to each interface.
<b>Net Mask</b>	The subnet mask.
<b>VLAN ID</b>	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

<i>Term</i>	<i>Definition</i>
<b>Mac Address</b>	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.
<b>VLAN ID</b>	There is a VLAN Identifier (VID) associated with each VLAN.

## 2.4 Double VLAN Commands

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

### 2.4.1 dvlan-tunnel ethertype

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



<b>Default</b>	vman
<b>Format</b>	<code>dvlan-tunnel ethertype {802.1Q   vman   custom} [0-65535]</code>
<b>Mode</b>	Global Config

## 2.4.2 mode dot1q-tunnel

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

<b>Default</b>	disabled
<b>Format</b>	<code>mode dot1q-tunnel</code>
<b>Mode</b>	Interface Config

### 2.4.2.1 no mode dot1q-tunnel

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

<b>Format</b>	<code>no mode dot1q-tunnel</code>
<b>Mode</b>	Interface Config

## 2.4.3 mode dvlan-tunnel

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



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

<b>Default</b>	disabled
<b>Format</b>	<code>mode dvlan-tunnel</code>
<b>Mode</b>	Interface Config

### 2.4.3.1 no mode dvlan-tunnel

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

<b>Format</b>	<code>no mode dvlan-tunnel</code>
<b>Mode</b>	Interface Config

## 2.4.4 show dot1q-tunnel

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

<b>Format</b>	<code>show dot1q-tunnel [interface {&lt;slot/port&gt;   all}]</code>
---------------	--



- Mode**
- Privileged EXEC
  - User EXEC

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Mode</b>	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
<b>EtherType</b>	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

### 2.4.5 show dvlan-tunnel

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

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

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Mode</b>	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
<b>EtherType</b>	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

## 2.5 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:

<i>Parameter</i>	<i>Description</i>
<b>vlan-id</b>	Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID's are from 1 to 4094 (the max supported by the platform).
<b>dot1p</b>	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.
<b>none</b>	Allow the IP phone to use its own configuration to send untagged voice traffic.
<b>untagged</b>	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.

<i>Term</i>	<i>Definition</i>
<b>Administrative Mode</b>	The Global Voice VLAN mode.

When the `interface` is specified:

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

## 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

<i>Term</i>	<i>Definition</i>
<b>Group ID</b>	The number that identifies the protected port group.
<b>Name</b>	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.
<b>List of Physical Ports</b>	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

<i>Term</i>	<i>Definition</i>
<b>Name</b>	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.
<b>Protected</b>	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

<i>Term</i>	<i>Definition</i>
<b>GMRP Admin Mode</b>	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
<b>GVRP Admin Mode</b>	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

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Join Timer</b>	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).
<b>Leave Timer</b>	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).
<b>LeaveAll Timer</b>	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).
<b>Port GMRP Mode</b>	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

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	The slot/port of the interface that this row in the table describes.



<b>Term</b>	<b>Definition</b>
<b>Join Timer</b>	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).
<b>Leave Timer</b>	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).
<b>LeaveAll Timer</b>	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).
<b>Port GMRP Mode</b>	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

<b>Term</b>	<b>Definition</b>
<b>Mac Address</b>	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.
<b>Type</b>	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.
<b>Description</b>	The text description of this multicast table entry.
<b>Interfaces</b>	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Fit:).

## 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-riden 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 maximum VLAN 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'. If the control mode is not 'auto' or 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.

**Default**           16  
**Format**            `dot1x max-users <count>`  
**Mode**             Interface Config

#### 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.

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

**Default** auto  
**Format** `dot1x port-control all {force-unauthorized | force-authorized | auto}`  
**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'. If the control mode is not 'auto' an error will be returned.

**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:

<b>Tokens</b>	<b>Definition</b>
<b>reauth-period</b>	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.
<b>quiet-period</b>	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.
<b>tx-period</b>	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.
<b>supp-timeout</b>	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.
<b>server-timeout</b>	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.

<b>Default</b>	0
<b>Format</b>	<code>dot1x unauthenticated-vlan &lt;vlan id&gt;</code>
<b>Mode</b>	Interface Config

#### 2.11.16.1 no dot1x unauthenticated-vlan

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

<b>Format</b>	<code>no dot1x unauthenticated-vlan</code>
<b>Mode</b>	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.

<b>Format</b>	<code>dot1x user &lt;user&gt; {&lt;slot/port&gt;   all}</code>
<b>Mode</b>	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.

<b>Format</b>	<code>no dot1x user &lt;user&gt; {&lt;slot/port&gt;   all}</code>
<b>Mode</b>	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.

<b>Format</b>	<code>users defaultlogin &lt;listname&gt;</code>
<b>Mode</b>	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

<i>Term</i>	<i>Definition</i>
<b>Authentication Login List</b>	The authentication login listname.
<b>Method 1</b>	The first method in the specified authentication login list, if any.
<b>Method 2</b>	The second method in the specified authentication login list, if any.
<b>Method 3</b>	The third method in the specified authentication login list, if any.

## 2.11.21        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

<i>Term</i>	<i>Definition</i>
<b>User</b>	The user assigned to the specified authentication login list.
<b>Component</b>	The component (User or 802.1x) for which the authentication login list is assigned.

## 2.11.22        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 `<slot/port>` or `<vlanid>`, the command displays the global dot1x mode and the VLAN Assignment mode.

<i>Term</i>	<i>Definition</i>
<b>Administrative Mode</b>	Indicates whether authentication control on the switch is enabled or disabled.



<b>Term</b>	<b>Definition</b>
<b>VLAN Assignment Mode</b>	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.

<b>Term</b>	<b>Definition</b>
<b>Interface</b>	The interface whose configuration is displayed.
<b>Control Mode</b>	The configured control mode for this port. Possible values are force-unauthorized   force-authorized   auto   authorized   unauthorized.
<b>Operating Control Mode</b>	The control mode under which this port is operating. Possible values are authorized   unauthorized.
<b>Reauthentication Enabled</b>	Indicates whether re-authentication is enabled on this port.
<b>Port Status</b>	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.

<b>Term</b>	<b>Definition</b>
<b>Port</b>	The interface whose configuration is displayed.
<b>Protocol Version</b>	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
<b>PAE Capabilities</b>	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
<b>Authenticator PAE State</b>	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
<b>Backend Authentication State</b>	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
<b>Quiet Period</b>	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.
<b>Transmit Period</b>	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.
<b>Guest-VLAN ID</b>	The guest VLAN identifier configured on the interface.
<b>Guest-Vlan Operational Mode</b>	Indicates whether guest-vlan operational mode is enabled or disabled.
<b>Supplicant Timeout</b>	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.
<b>Server Timeout</b>	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.
<b>Maximum Requests</b>	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.
<b>Vlan-assigned</b>	The VLAN assigned to the port by the radius server.



<i>Term</i>	<i>Definition</i>
<b>Reauthentication Period</b>	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.
<b>Reauthentication Enabled</b>	Indicates if reauthentication is enabled on this port. Possible values are "True" or "False".
<b>Key Transmission Enabled</b>	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
<b>Control Direction</b>	The control direction for the specified port or ports. Possible values are both or in.

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

<i>Term</i>	<i>Definition</i>
<b>Port</b>	The interface whose statistics are displayed.
<b>EAPOL Frames Received</b>	The number of valid EAPOL frames of any type that have been received by this authenticator.
<b>EAPOL Frames Transmitted</b>	The number of EAPOL frames of any type that have been transmitted by this authenticator.
<b>EAPOL Start Frames Received</b>	The number of EAPOL start frames that have been received by this authenticator.
<b>EAPOL Logoff Frames Received</b>	The number of EAPOL logoff frames that have been received by this authenticator.
<b>Last EAPOL Frame Version</b>	The protocol version number carried in the most recently received EAPOL frame.
<b>Last EAPOL Frame Source</b>	The source MAC address carried in the most recently received EAPOL frame.
<b>EAP Response/Id Frames Received</b>	The number of EAP response/identity frames that have been received by this authenticator.
<b>EAP Response Frames Received</b>	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
<b>EAP Request/Id Frames Transmitted</b>	The number of EAP request/identity frames that have been transmitted by this authenticator.
<b>EAP Request Frames Transmitted</b>	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
<b>Invalid EAPOL Frames Received</b>	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
<b>EAP Length Error Frames Received</b>	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

### 2.11.23 show dot1x clients

This command displays 802.1x client information.

**Format**            `show dot1x clients {<slot/port> | all}`  
**Mode**              Privileged EXEC



<i>Term</i>	<i>Definition</i>
<b>Logical Interface</b>	The logical port number associated with a client.
<b>Interface</b>	The physical port to which the supplicant is associated.
<b>User Name</b>	The user name used by the client to authenticate to the server.
<b>Supplicant MAC Address</b>	The supplicant device MAC address.
<b>Session Time</b>	The time since the supplicant is logged on.
<b>Filter ID</b>	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
<b>VLAN ID</b>	The VLAN assigned to the port.
<b>VLAN Assigned</b>	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 PVID of the port was that VLAN ID.
<b>Session Timeout</b>	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.
<b>Session Termination Action</b>	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.

#### 2.11.24 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

<i>Term</i>	<i>Definition</i>
<b>Users</b>	Users configured locally to have access to the specified port.

#### 2.11.25 show users authentication

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

**Format**      `show users authentication`  
**Mode**        Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>User</b>	Lists every user that has an authentication login list assigned.
<b>System Login</b>	The authentication login list assigned to the user for system login.
<b>802.1x Port Security</b>	The authentication login list assigned to the user for 802.1x port security.



## 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 storm 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.

<b>Default</b>	disabled
<b>Format</b>	<code>storm-control broadcast</code>
<b>Mode</b>	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.

<b>Format</b>	<code>no storm-control broadcast</code>
<b>Mode</b>	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 multicast all rate

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 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

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

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 show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **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
<b>Bcast Mode</b>	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
<b>Bcast Level</b>	The broadcast storm control level.
<b>Mcast Mode</b>	Shows whether the multicast storm control mode is enabled or disabled.
<b>Mcast Level</b>	The multicast storm control level.
<b>Ucast Mode</b>	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
<b>Ucast Level</b>	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
```

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

Intf	Bcast Mode	Bcast Level	Mcast Mode	Mcast Level	Ucast Mode	Ucast 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%





## 2.13 Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel.

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 4.6.6 “clear port-channel” on page 4 - 27.

**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 LACPDU. 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 to configure the default administrative values of actor state as transmitted by the Actor in LACPDU.

**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 to 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

**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 **a11** sets every configured port-channel with the same administrative mode setting.

**Format**            `port-channel adminmode [a11]`  
**Mode**             Global Config

### 2.13.30.1 no port-channel adminmode

This command disables a port-channel (LAG). The option **a11** sets every configured port-channel with the same administrative mode setting.

**Format**            `no port-channel adminmode [a11]`  
**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

<b>Term</b>	<b>Definition</b>
<b>1</b>	Source MAC, VLAN, EtherType, and incoming port associated with the packet
<b>2</b>	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
<b>3</b>	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
<b>4</b>	Source IP and Source TCP/UDP fields of the packet
<b>5</b>	Destination IP and Destination TCP/UDP Port fields of the packet
<b>6</b>	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
<b>&lt;slot/port&gt;  all</b>	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.

<i>Parameter</i>	<i>Description</i>
<b>System Priority</b>	The administrative value of the Key.
<b>Actor Admin Key</b>	The administrative value of the Key.
<b>Port Priority</b>	The priority value assigned to the Aggregation Port.
<b>Admin State</b>	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.

<i>Parameter</i>	<i>Description</i>
<b>System Priority</b>	The administrative value of priority associated with the Partner's System ID.
<b>System-ID</b>	The value representing the administrative value of the Aggregation Port's protocol Partner's System ID.
<b>Admin Key</b>	The administrative value of the Key for the protocol Partner.
<b>Port Priority</b>	The administrative value of the Key for protocol Partner.
<b>Port-ID</b>	The administrative value of the port number for the protocol Partner.
<b>Admin State</b>	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:

<i>Term</i>	<i>Definition</i>
<b>Logical Interface</b>	The slot/port of the logical interface.
<b>Port-channel Name</b>	The name of port-channel (LAG) interface.
<b>Link-State</b>	Shows whether the link is up or down.
<b>Trap Flag</b>	Shows whether trap flags are enabled or disabled.
<b>Type</b>	Shows whether the port-channel is statically or dynamically maintained.
<b>Mbr Ports</b>	The members of this port-channel.
<b>Active Ports</b>	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

<i>Term</i>	<i>Definition</i>
<b>Logical Interface</b>	Valid slot and port number separated by a forward slash.
<b>Port-Channel Name</b>	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
<b>Link State</b>	Indicates whether the Link is up or down.
<b>Admin Mode</b>	May be enabled or disabled. The factory default is enabled.
<b>Mbr Ports</b>	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).
<b>Device Timeout</b>	For each port, lists the timeout ( <b>long</b> or <b>short</b> ) for Device Type ( <b>actor</b> or <b>partner</b> ).
<b>Port Speed</b>	Speed of the port-channel port.
<b>Type</b>	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. <ul style="list-style-type: none"> <li>• <b>Static</b> - The port-channel is statically maintained.</li> <li>• <b>Dynamic</b> - The port-channel is dynamically maintained.</li> </ul>
<b>Active Ports</b>	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 enable 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

<i>Term</i>	<i>Definition</i>
<b>Session ID</b>	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.





Term	Definition
<b>Monitor Session Mode</b>	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <i>&lt;session-id&gt;</i> . The possible values are Enabled and Disabled.
<b>Probe Port</b>	Probe port (destination port) for the session identified with <i>&lt;session-id&gt;</i> . If probe port is not set then this field is blank.
<b>Source Port</b>	The port, which is configured as mirrored port (source port) for the session identified with <i>&lt;session-id&gt;</i> . If no source port is configured for the session then this field is blank.
<b>Type</b>	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>`  
**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>`  
**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>`  
**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>`  
**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

<b>Term</b>	<b>Definition</b>
<b>MAC Address</b>	The MAC Address of the static MAC filter entry.
<b>VLAN ID</b>	The VLAN ID of the static MAC filter entry.
<b>Source Port(s)</b>	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

<i>Term</i>	<i>Definition</i>
<b>Mac Address</b>	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.
<b>Type</b>	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.
<b>Description</b>	The text description of this multicast table entry.
<b>Interfaces</b>	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

## 2.16 DHCP Snooping Configuration Commands

This section describes commands you use to configure DHCP Snooping.

### 2.16.1 ip dhcp snooping

Use this command to enable DHCP Snooping globally.

**Default** disabled

**Format** `ip dhcp snooping`

**Mode** Global Config

#### 2.16.1.1 no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

**Format** `no ip dhcp snooping`

**Mode** Global Config

### 2.16.2 ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

**Default** disabled

**Format** `ip dhcp snooping vlan <vlan-list>`

**Mode** Global Config



### 2.16.2.1 no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

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

### 2.16.3 ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DHCP message.

**Default** enabled  
**Format** ip dhcp snooping verify mac-address  
**Mode** Global Config

### 2.16.3.1 no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

**Format** no ip dhcp snooping verify mac-address  
**Mode** Global Config

### 2.16.4 ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

**Default** local  
**Format** ip dhcp snooping database {local|tftp://hostIP/filename}  
**Mode** Global Config

### 2.16.5 ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

**Default** 300 seconds  
**Format** ip dhcp snooping database write-delay <in seconds>  
**Mode** Global Config

### 2.16.5.1 no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

**Format** no ip dhcp snooping database write-delay  
**Mode** Global Config



## 2.16.6 ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

**Format** `ip dhcp snooping binding <mac-address> vlan <vlan id> <ip address>  
interface <interface id>`

**Mode** Global Config

### 2.16.6.1 no ip dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

**Format** `no ip dhcp snooping binding <mac-address>`

**Mode** Global Config

## 2.16.7 ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

**Format** `ip verify binding <mac-address> vlan <vlan id> <ip address> interface  
<interface id>`

**Mode** Global Config

### 2.16.7.1 no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

**Format** `no ip verify binding <mac-address> vlan <vlan id> <ip address> interface  
<interface id>`

**Mode** Global Config

## 2.16.8 ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come. The default rate is 15 pps with a range from 0 to 30 pps. The default burst level is 1 second with a range of 1 to 15 seconds.

**Default** 15 pps for rate limiting and 1 sec for burst interval

**Format** `ip dhcp snooping limit {rate pps [burst interval seconds]}`

**Mode** Interface Config

### 2.16.8.1 no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

**Format** `no ip dhcp snooping limit`

**Mode** Interface Config



## 2.16.9 ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application.

<b>Default</b>	disabled
<b>Format</b>	<code>ip dhcp snooping log-invalid</code>
<b>Mode</b>	Interface Config

### 2.16.9.1 no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

<b>Format</b>	<code>no ip dhcp snooping log-invalid</code>
<b>Mode</b>	Interface Config

## 2.16.10 ip dhcp snooping trust

Use this command to configure the port as trusted.

<b>Default</b>	disabled
<b>Format</b>	<code>ip dhcp snooping trust</code>
<b>Mode</b>	Interface Config

### 2.16.10.1 no ip dhcp snooping trust

Use this command to configure the port as untrusted.

<b>Format</b>	<code>no ip dhcp snooping trust</code>
<b>Mode</b>	Interface Config

## 2.16.11 ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the “port-security” option, the data traffic will be filtered based on the IP and MAC addresses.

<b>Default</b>	the source ID is the IP address
<b>Format</b>	<code>ip verify source {port-security}</code>
<b>Mode</b>	Interface Config

### 2.16.11.1 no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

<b>Format</b>	<code>no ip verify source</code>
<b>Mode</b>	Interface Config



## 2.16.12 show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

**Format**        `show ip dhcp snooping`

**Mode**

- Privileged EXEC
- User EXEC

<b>Term</b>	<b>Definition</b>
<b>Interface</b>	The interface for which data is displayed.
<b>Trusted</b>	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
<b>Log Invalid Pkts</b>	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

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

```
(switch) #show ip dhcp snooping
```

```
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40
```

Interface	Trusted	Log Invalid Pkts
0/1	Yes	No
0/2	No	Yes
0/3	No	Yes
0/4	No	No
0/6	No	No

## 2.16.13 show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- **Dynamic:** Restrict the output based on DHCP snooping.
- **Interface:** Restrict the output based on a specific interface.
- **Static:** Restrict the output based on static entries.
- **VLAN:** Restrict the output based on VLAN.

**Format**        `show ip dhcp snooping binding [{static/dynamic}] [interface slot/port] [vlan id]`

**Mode**

- Privileged EXEC
- User EXEC

<b>Term</b>	<b>Definition</b>
<b>MAC Address</b>	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
<b>IP Address</b>	Displays the valid IP address for the binding rule.
<b>VLAN</b>	The VLAN for the binding rule.
<b>Interface</b>	The interface to add a binding into the DHCP snooping interface.





<b>Term</b>	<b>Definition</b>
<b>Type</b>	Binding type; statically configured from the CLI or dynamically learned.
<b>Lease (sec)</b>	The remaining lease time for the entry.

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

```
(switch) #show ip dhcp snooping binding
```

Total number of bindings: 2

MAC Address	IP Address	VLAN	Interface	Type	Lease (Secs)
00:02:B3:06:60:80	210.1.1.3	10	0/1		86400
00:0F:FE:00:13:04	210.1.1.4	10	0/1		86400

### 2.16.14 show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

**Format** `show ip dhcp snooping database`

**Mode**

- Privileged EXEC
- User EXEC

<b>Term</b>	<b>Definition</b>
<b>Agent URL</b>	Bindings database agent URL.
<b>Write Delay</b>	The maximum write time to write the database into local or remote.

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

```
(switch) #show ip dhcp snooping database
```

```
agent url: /10.131.13.79:/sail.txt
```

```
write-delay: 5000
```

### 2.16.15 show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

**Format** `show ip dhcp snooping statistics`

**Mode**

- Privileged EXEC
- User EXEC

<b>Term</b>	<b>Definition</b>
<b>Interface</b>	The IP address of the interface in slot/port format.
<b>MAC Verify Failures</b>	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.
<b>Client Ifc Mismatch</b>	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.



<i>Term</i>	<i>Definition</i>
<b>DHCP Server Msgs Rec'd</b>	Represents the number of DHCP server messages received on Untrusted ports.

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

```
(switch) #show ip dhcp snooping statistics
```

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Rec'd
1/0/2	0	0	0
1/0/3	0	0	0
1/0/4	0	0	0
1/0/5	0	0	0
1/0/6	0	0	0
1/0/7	0	0	0
1/0/8	0	0	0
1/0/9	0	0	0
1/0/10	0	0	0
1/0/11	0	0	0
1/0/12	0	0	0
1/0/13	0	0	0
1/0/14	0	0	0
1/0/15	0	0	0
1/0/16	0	0	0
1/0/17	0	0	0
1/0/18	0	0	0
1/0/19	0	0	0
1/0/20	0	0	0

### 2.16.16 clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

**Format** `clear ip dhcp snooping binding [interface <slot/port>]`

- Mode**
- Privileged EXEC
  - User EXEC

### 2.16.17 clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

**Format** `clear ip dhcp snooping statistics`

- Mode**
- Privileged EXEC
  - User EXEC

### 2.16.18 show ip verify source

Use this command to display the IPSPG configurations on all ports.

**Format** `show ip verify source`



- Mode**
- Privileged EXEC
  - User EXEC

<b>Term</b>	<b>Definition</b>
<b>Interface</b>	Interface address in slot/port format.
<b>Filter Type</b>	Is one of two values: <ul style="list-style-type: none"> <li>• ip-mac: User has configured MAC address filtering on this interface.</li> <li>• ip: Only IP address filtering on this interface.</li> </ul>
<b>IP Address</b>	IP address of the interface
<b>MAC Address</b>	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays "permit-all."
<b>VLAN</b>	The VLAN for the binding rule.

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

```
(switch) #show ip verify source
```

Interface	Filter Type	IP Address	MAC Address	Vlan
0/1	ip-mac	210.1.1.3	00:02:B3:06:60:80	10
0/1	ip-mac	210.1.1.4	00:0F:FE:00:13:04	10

### 2.16.19 show ip source binding

Use this command to display the IPSG bindings.

- Format** `show ip source binding [{static/dynamic}] [interface slot/port] [vlan id]`
- Mode**
- Privileged EXEC
  - User EXEC

<b>Term</b>	<b>Definition</b>
<b>MAC Address</b>	The MAC address for the entry that is added.
<b>IP Address</b>	The IP address of the entry that is added.
<b>Type</b>	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
<b>VLAN</b>	VLAN for the entry.
<b>Interface</b>	IP address of the interface in slot/port format.

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

```
(switch) #show ip source binding
```

MAC Address	IP Address	Type	Vlan	Interface
00:00:00:00:00:08	1.2.3.4	dhcp-snooping	2	1/0/1
00:00:00:00:00:09	1.2.3.4	dhcp-snooping	3	1/0/1
00:00:00:00:00:0A	1.2.3.4	dhcp-snooping	4	1/0/1



## 2.17 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.

### 2.17.1 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

#### 2.17.1.1 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

### 2.17.2 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

#### 2.17.2.1 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

### 2.17.3 ip arp inspection vlan logging

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



<b>Default</b>	enabled
<b>Format</b>	<code>ip arp inspection vlan vlan-list logging</code>
<b>Mode</b>	Global Config

### 2.17.3.1 no ip arp inspection vlan logging

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

<b>Format</b>	<code>no ip arp inspection vlan vlan-list logging</code>
<b>Mode</b>	Global Config

## 2.17.4 ip arp inspection trust

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

<b>Default</b>	enabled
<b>Format</b>	<code>ip arp inspection trust</code>
<b>Mode</b>	Interface Config

### 2.17.4.1 no ip arp inspection trust

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

<b>Format</b>	<code>no ip arp inspection trust</code>
<b>Mode</b>	Interface Config

## 2.17.5 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.



**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.

<b>Default</b>	15 pps for rate and 1 second for burst-interval
<b>Format</b>	<code>ip arp inspection limit {rate pps [burst interval seconds]   none}</code>
<b>Mode</b>	Interface Config

### 2.17.5.1 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.

<b>Format</b>	<code>no ip arp inspection limit</code>
<b>Mode</b>	Interface Config



## 2.17.6 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

### 2.17.6.1 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

## 2.17.7 arp access-list

Use this command to create an ARP ACL.

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

### 2.17.7.1 no arp access-list

Use this command to delete a configured ARP ACL.

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

## 2.17.8 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

### 2.17.8.1 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



### 2.17.9 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

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

### 2.17.10 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



<i>Term</i>	<i>Definition</i>
<b>VLAN</b>	The VLAN ID for each displayed row.
<b>Forwarded</b>	The total number of valid ARP packets forwarded in this VLAN.
<b>Dropped</b>	The total number of not valid ARP packets dropped in this VLAN.
<b>DHCP Drops</b>	The number of packets dropped due to DHCP snooping binding database match failure.
<b>ACL Drops</b>	The number of packets dropped due to ARP ACL rule match failure.
<b>DHCP Permits</b>	The number of packets permitted due to DHCP snooping binding database match.
<b>ACL Permits</b>	The number of packets permitted due to ARP ACL rule match.
<b>Bad Src MAC</b>	The number of packets dropped due to Source MAC validation failure.
<b>Bad Dest MAC</b>	The number of packets dropped due to Destination MAC validation failure.
<b>Invalid IP</b>	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 Drops	ACL Drops	DHCP Permits	ACL Permits	Bad Src MAC	Bad Dest MAC	Invalid IP
10	11	1	65	25	1	1	0
20	1	0	8	2	0	1	1

## 2.17.11 clear ip arp inspection statistics

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

<b>Default</b>	none
<b>Format</b>	<b>clear ip arp inspection statistics</b>
<b>Mode</b>	Privileged EXEC

## 2.17.12 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.

<b>Format</b>	<b>show ip arp inspection interfaces [slot/port]</b>
<b>Mode</b>	<ul style="list-style-type: none"> <li>Privileged EXEC</li> <li>User EXEC</li> </ul>





<b>Term</b>	<b>Definition</b>
<b>Interface</b>	The interface ID for each displayed row.
<b>Trust State</b>	Whether the interface is trusted or untrusted for DAI.
<b>Rate Limit</b>	The configured rate limit value in packets per second.
<b>Burst Interval</b>	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
```

### 2.17.13 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
```

## 2.18 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.

### 2.18.1 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

### 2.18.1.1 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

## 2.18.2 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

### 2.18.2.1 no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

**Format** `no set igmp interfacemode`  
**Mode** Global Config



### 2.18.3 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

#### 2.18.3.1 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

### 2.18.4 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

#### 2.18.4.1 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

### 2.18.5 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

#### 2.18.5.1 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

### 2.18.6 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



### 2.18.6.1 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

### 2.18.7 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

### 2.18.7.1 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

### 2.18.8 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

### 2.18.8.1 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

### 2.18.9 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:

<b>Term</b>	<b>Definition</b>
<b>Admin Mode</b>	Indicates whether or not IGMP Snooping is active on the switch.
<b>Multicast Control Frame Count</b>	The number of multicast control frames that are processed by the CPU.
<b>Interface Enabled for IGMP Snooping</b>	The list of interfaces on which IGMP Snooping is enabled.
<b>VLANS Enabled for IGMP Snooping</b>	The list of VLANS on which IGMP Snooping is enabled.

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

<b>Term</b>	<b>Definition</b>
<b>IGMP Snooping Admin Mode</b>	Indicates whether IGMP Snooping is active on the interface.
<b>Fast Leave Mode</b>	Indicates whether IGMP Snooping Fast-leave is active on the interface.
<b>Group Membership Interval</b>	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.
<b>Maximum Response Time</b>	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.
<b>Multicast Router Expiry Time</b>	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:

<b>Term</b>	<b>Definition</b>
<b>VLAN ID</b>	The VLAN ID.
<b>IGMP Snooping Admin Mode</b>	Indicates whether IGMP Snooping is active on the VLAN.
<b>Fast Leave Mode</b>	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
<b>Group Membership Interval</b>	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.
<b>Maximum Response Time</b>	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.
<b>Multicast Router Expiry Time</b>	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.

### 2.18.10 show igmpsnooping mrouter interface

This command displays information about statically configured ports.

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



<b>Term</b>	<b>Definition</b>
<b>Interface</b>	The port on which multicast router information is being displayed.
<b>Multicast Router Attached</b>	Indicates whether multicast router is statically enabled on the interface.
<b>VLAN ID</b>	The list of VLANs of which the interface is a member.

### 2.18.11 show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

<b>Format</b>	<code>show igmpsnooping mrouter vlan &lt;slot/port&gt;</code>
<b>Mode</b>	Privileged EXEC

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

### 2.18.12 show mac-address-table igmpsnooping

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

<b>Format</b>	<code>show mac-address-table igmpsnooping</code>
<b>Mode</b>	Privileged EXEC

<b>Term</b>	<b>Definition</b>
<b>MAC Address</b>	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.
<b>Type</b>	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).
<b>Description</b>	The text description of this multicast table entry.
<b>Interfaces</b>	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Fit:).

## 2.19 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.



### 2.19.1 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.

<b>Default</b>	disabled
<b>Format</b>	<code>set igmp querier [&lt;vlan-id&gt;] [address ipv4_address]</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• VLAN Mode</li></ul>

#### 2.19.1.1 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.

<b>Format</b>	<code>no set igmp querier [&lt;vlan-id&gt;] [address]</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• VLAN Mode</li></ul>

### 2.19.2 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.

<b>Default</b>	disabled
<b>Format</b>	<code>set igmp querier query-interval &lt;1-18000&gt;</code>
<b>Mode</b>	Global Config

#### 2.19.2.1 no set igmp querier query-interval

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

<b>Format</b>	<code>no set igmp querier query-interval</code>
<b>Mode</b>	Global Config





### 2.19.3 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

#### 2.19.3.1 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

### 2.19.4 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

#### 2.19.4.1 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

### 2.19.5 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

#### 2.19.5.1 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



## 2.19.6 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.

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

<i>Field</i>	<i>Description</i>
<b>VLAN Admin Mode</b>	Indicates whether iGMP Snooping Querier is active on the VLAN.
<b>VLAN Operational State</b>	Indicates whether IGMP Snooping Querier is in "Querier" or "Non-Querier" state. When the switch is in <i>Querier</i> state, it will send out periodic general queries. When in <i>Non-Querier</i> state, it will wait for moving to Querier state and does not send out any queries.
<b>VLAN Operational Max Response Time</b>	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.
<b>Querier Election Participation</b>	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
<b>Querier VLAN Address</b>	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.
<b>Operational Version</b>	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
<b>Last Querier Address</b>	Indicates the IP address of the most recent Querier from which a Query was received.
<b>Last Querier Version</b>	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.

## 2.20 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.



## 2.20.1 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.

<b>Default</b>	disabled
<b>Format</b>	<code>set mld &lt;vlanid&gt;</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• Interface Config</li><li>• VLAN Mode</li></ul>

### 2.20.1.1 no set mld

Use this command to disable MLD Snooping on the system.

<b>Format</b>	<code>set mld &lt;vlanid&gt;</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• Interface Config</li><li>• VLAN Mode</li></ul>

## 2.20.2 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.

<b>Default</b>	disabled
<b>Format</b>	<code>set mld interfacemode</code>
<b>Mode</b>	Global Config

### 2.20.2.1 no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

<b>Format</b>	<code>no set mld interfacemode</code>
<b>Mode</b>	Global Config



### 2.20.3 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.

<b>Default</b>	disabled
<b>Format</b>	<b>set mld fast-leave</b> <vlanid>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Interface Config</li><li>• VLAN Mode</li></ul>

#### 2.20.3.1 no set mld fast-leave

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

<b>Format</b>	<b>no set mld fast-leave</b> <vlanid>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Interface Config</li><li>• VLAN Mode</li></ul>

### 2.20.4 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.

<b>Default</b>	260 seconds
<b>Format</b>	<b>set mld groupmembership-interval</b> <vlanid> <2-3600>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Interface Config</li><li>• Global Config</li><li>• VLAN Mode</li></ul>

#### 2.20.4.1 no set groupmembership-interval

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

<b>Format</b>	<b>no set mld groupmembership-interval</b>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Interface Config</li><li>• Global Config</li><li>• VLAN Mode</li></ul>



## 2.20.5 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.

<b>Default</b>	10 seconds
<b>Format</b>	<code>set mld maxresponse &lt;1-65&gt;</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• Interface Config</li><li>• VLAN Mode</li></ul>

### 2.20.5.1 no set mld maxresponse

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

<b>Format</b>	<code>no set mld maxresponse</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• Interface Config</li><li>• VLAN Mode</li></ul>

## 2.20.6 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.

<b>Default</b>	0
<b>Format</b>	<code>set mld mcrtexpiretime &lt;vlanid&gt; &lt;0-3600&gt;</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• Interface Config</li></ul>

### 2.20.6.1 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.

<b>Format</b>	<code>no set mld mcrtexpiretime &lt;vlanid&gt;</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• Interface Config</li></ul>

## 2.20.7 set mld mrouter

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

<b>Format</b>	<code>set mld mrouter &lt;vlanid&gt;</code>
<b>Mode</b>	Interface Config



### 2.20.7.1 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

### 2.20.8 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

### 2.20.8.1 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

### 2.20.9 show mldsnoothing

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

**Format** `show mldsnoothing [<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.

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

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

<b>Term</b>	<b>Definition</b>
<b>MLD Snooping Admin Mode</b>	Indicates whether MLD Snooping is active on the interface.
<b>Fast Leave Mode</b>	Indicates whether MLD Snooping Fast Leave is active on the VLAN.



<b>Term</b>	<b>Definition</b>
<b>Group Membership Interval</b>	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.
<b>Max Response Time</b>	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.
<b>Multicast Router Present Expiration Time</b>	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.

<b>Term</b>	<b>Definition</b>
<b>VLAN Admin Mode</b>	Indicates whether MLD Snooping is active on the VLAN.

### 2.20.10 show mldsnoping mrouter interface

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

**Format**            `show mldsnoping mrouter interface <unit/slot/port>`  
**Mode**                Privileged EXEC

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

### 2.20.11 show mldsnoping mrouter vlan

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

**Format**            `show mldsnoping mrouter vlan <unit/slot/port>`  
**Mode**                Privileged EXEC

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

### 2.20.12 show mac-address-table mldsnoping

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

**Format**            `show mac-address-table mldsnoping`  
**Mode**                Privileged EXEC



<b>Term</b>	<b>Definition</b>
<b>MAC Address</b>	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.
<b>Type</b>	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.)
<b>Description</b>	The text description of this multicast table entry.
<b>Interfaces</b>	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

## 2.21 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.

### 2.21.1 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.

<b>Default</b>	disabled
<b>Format</b>	<code>set mld querier [&lt;vlan-id&gt;] [address ipv6_address]</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Global Config</li> <li>• VLAN Mode</li> </ul>

#### 2.21.1.1 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.

<b>Format</b>	<code>no set mld querier [&lt;vlan-id&gt;] [address]</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Global Config</li> <li>• VLAN Mode</li> </ul>

### 2.21.2 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

#### 2.21.2.1 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

### 2.21.3 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

#### 2.21.3.1 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

### 2.21.4 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

#### 2.21.4.1 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



### 2.21.5 show mldsnoothing querier

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

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

**Mode** Privileged EXEC

When the optional arguments `<vlanid>` are not used, the command displays the following information.

Field	Description
<b>Admin Mode</b>	Indicates whether or not MLD Snooping Querier is active on the switch.
<b>Admin Version</b>	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to <code>MLD v1</code> and it cannot be changed.
<b>Querier Address</b>	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.
<b>Query Interval</b>	Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
<b>Querier Timeout</b>	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
<b>VLAN Admin Mode</b>	Indicates whether MLD Snooping Querier is active on the VLAN.
<b>VLAN Operational State</b>	Indicates whether MLD Snooping Querier is in <i>Querier</i> or <i>Non-Querier</i> state. When the switch is in <i>Querier</i> state, it will send out periodic general queries. When in <i>Non-Querier</i> state, it will wait for moving to <i>Querier</i> state and does not send out any queries.
<b>VLAN Operational Max Response Time</b>	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.
<b>Querier Election Participate</b>	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
<b>Querier VLAN Address</b>	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.
<b>Operational Version</b>	This version of IPv6 will be used while sending out MLD queriers on this VLAN.
<b>Last Querier Address</b>	Indicates the IP address of the most recent Querier from which a Query was received.
<b>Last Querier Version</b>	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.



## 2.22 Port Security Commands

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



**Note:** To enable the SNMP trap specific to port security, see 5.8.7 “snmp-server enable traps violation” on page 5 - 23.

### 2.22.1 port-security

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

<b>Default</b>	disabled
<b>Format</b>	<code>port-security</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• Interface Config</li></ul>

#### 2.22.1.1 no port-security

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

<b>Format</b>	<code>no port-security</code>
<b>Mode</b>	<ul style="list-style-type: none"><li>• Global Config</li><li>• Interface Config</li></ul>

### 2.22.2 port-security max-dynamic

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

<b>Default</b>	600
<b>Format</b>	<code>port-security max-dynamic &lt;maxvalue&gt;</code>
<b>Mode</b>	Interface Config

#### 2.22.2.1 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.

<b>Format</b>	<code>no port-security max-dynamic</code>
<b>Mode</b>	Interface Config

### 2.22.3 port-security max-static

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

<b>Default</b>	20
<b>Format</b>	<code>port-security max-static &lt;maxvalue&gt;</code>
<b>Mode</b>	Interface Config



### 2.22.3.1 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

### 2.22.4 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

### 2.22.4.1 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

### 2.22.5 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

### 2.22.6 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

<i>Term</i>	<i>Definition</i>
<b>Admin Mode</b>	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:

<i>Term</i>	<i>Definition</i>
<b>Admin Mode</b>	Port Locking mode for the Interface.
<b>Dynamic Limit</b>	Maximum dynamically allocated MAC Addresses.
<b>Static Limit</b>	Maximum statically allocated MAC Addresses.
<b>Violation Trap Mode</b>	Whether violation traps are enabled.



### 2.22.7 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

<i>Term</i>	<i>Definition</i>
<b>MAC Address</b>	MAC Address of dynamically locked MAC.

### 2.22.8 show port-security static

This command displays the statically locked MAC addresses for port.

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

**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>MAC Address</b>	MAC Address of statically locked MAC.

### 2.22.9 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

<i>Term</i>	<i>Definition</i>
<b>MAC Address</b>	MAC Address of discarded packet on locked port.

## 2.23 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.

### 2.23.1 lldp transmit

Use this command to enable the LLDP advertise capability.

**Default** disabled

**Format** `lldp transmit`

**Mode** Interface Config



### 2.23.1.1 no lldp transmit

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

**Format** no lldp transmit

**Mode** Interface Config

### 2.23.2 lldp receive

Use this command to enable the LLDP receive capability.

**Default** disabled

**Format** lldp receive

**Mode** Interface Config

### 2.23.2.1 no lldp receive

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

**Format** no lldp receive

**Mode** Interface Config

### 2.23.3 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

### 2.23.3.1 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

### 2.23.4 lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use *sys-name* to transmit the system name TLV. To configure the system name, see 5.8.1 “snmp-server” on page 5 - 21. 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

#### 2.23.4.1 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

### 2.23.5 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

#### 2.23.5.1 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

### 2.23.6 lldp notification

Use this command to enable remote data change notifications.

**Default** disabled  
**Format** `lldp notification`  
**Mode** Interface Config

#### 2.23.6.1 no lldp notification

Use this command to disable notifications.

**Default** disabled  
**Format** `no lldp notification`  
**Mode** Interface Config



### 2.23.7 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

#### 2.23.7.1 no lldp notification-interval

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

**Format** `no lldp notification-interval`  
**Mode** Global Config

### 2.23.8 clear lldp statistics

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

**Format** `clear lldp statistics`  
**Mode** Privileged Exec

### 2.23.9 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

### 2.23.10 show lldp

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

**Format** `show lldp`  
**Mode** Privileged Exec

<i>Term</i>	<i>Definition</i>
<b>Transmit Interval</b>	How frequently the system transmits local data LLDPDUs, in seconds.
<b>Transmit Hold Multiplier</b>	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
<b>Re-initialization Delay</b>	The delay before re-initialization, in seconds.
<b>Notification Interval</b>	How frequently the system sends remote data change notifications, in seconds.





### 2.23.11 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

<b>Term</b>	<b>Definition</b>
<b>Interface</b>	The interface in a slot/port format.
<b>Link</b>	Shows whether the link is up or down.
<b>Transmit</b>	Shows whether the interface transmits LLDPDUs.
<b>Receive</b>	Shows whether the interface receives LLDPDUs.
<b>Notify</b>	Shows whether the interface sends remote data change notifications.
<b>TLVs</b>	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).
<b>Mgmt</b>	Shows whether the interface transmits system management address information in the LLDPDUs.

### 2.23.12 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

<b>Term</b>	<b>Definition</b>
<b>Last Update</b>	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
<b>Total Inserts</b>	Total number of inserts to the remote data table.
<b>Total Deletes</b>	Total number of deletes from the remote data table.
<b>Total Drops</b>	Total number of times the complete remote data received was not inserted due to insufficient resources.
<b>Total Ageouts</b>	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:

<b>Term</b>	<b>Definition</b>
<b>Interface</b>	The interface in slot/port format.
<b>Transmit Total</b>	Total number of LLDP packets transmitted on the port.
<b>Receive Total</b>	Total number of LLDP packets received on the port.
<b>Discards</b>	Total number of LLDP frames discarded on the port for any reason.
<b>Errors</b>	The number of invalid LLDP frames received on the port.
<b>Ageouts</b>	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
<b>TVL Discards</b>	The number of TLVs discarded.
<b>TVL Unknowns</b>	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.



### 2.23.13 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
<b>Local Interface</b>	The interface that received the LLDPDU from the remote device.
<b>Chassis ID</b>	The ID of the remote device.
<b>Port ID</b>	The port number that transmitted the LLDPDU.
<b>System Name</b>	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
```

### 2.23.14 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
<b>Local Interface</b>	The interface that received the LLDPDU from the remote device.



<b>Term</b>	<b>Definition</b>
<b>Chassis ID Subtype</b>	The type of identification used in the Chassis ID field.
<b>Chassis ID</b>	The chassis of the remote device.
<b>Port ID Subtype</b>	The type of port on the remote device.
<b>Port ID</b>	The port number that transmitted the LLDPDU.
<b>System Name</b>	The system name of the remote device.
<b>System Description</b>	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
<b>Port Description</b>	Describes the port in an alpha-numeric format. The port description is configurable.
<b>System Capabilities Supported</b>	Indicates the primary function(s) of the device.
<b>System Capabilities Enabled</b>	Shows which of the supported system capabilities are enabled.
<b>Management Address</b>	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.
<b>Time To Live</b>	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

**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
```

### 2.23.15 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

<b>Term</b>	<b>Definition</b>
<b>Interface</b>	The interface in a slot/port format.



<i>Term</i>	<i>Definition</i>
<b>Port ID</b>	The port ID associated with this interface.
<b>Port Description</b>	The port description associated with the interface.

### 2.23.16 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

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	The interface that sends the LLDPDU.
<b>Chassis ID Subtype</b>	The type of identification used in the Chassis ID field.
<b>Chassis ID</b>	The chassis of the local device.
<b>Port ID Subtype</b>	The type of port on the local device.
<b>Port ID</b>	The port number that transmitted the LLDPDU.
<b>System Name</b>	The system name of the local device.
<b>System Description</b>	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
<b>Port Description</b>	Describes the port in an alpha-numeric format.
<b>System Capabilities Supported</b>	Indicates the primary function(s) of the device.
<b>System Capabilities Enabled</b>	Shows which of the supported system capabilities are enabled.
<b>Management Address</b>	The type of address and the specific address the local LLDP agent uses to send and receive information.

## 2.24 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.

### 2.24.1 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



### 2.24.1.1 no lldp med

Use this command to disable MED.

**Format** no lldp med  
**Mode** Interface Config

### 2.24.2 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

### 2.24.2.1 no lldp med confignotification

Use this command to disable notifications.

**Format** no lldp med confignotification  
**Mode** Interface Config

### 2.24.3 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

<b>Term</b>	<b>Definition</b>
<b>capabilities</b>	Transmit the LLDP capabilities TLV.
<b>ex-pd</b>	Transmit the LLDP extended PD TLV.
<b>ex-pse</b>	Transmit the LLDP extended PSE TLV.
<b>inventory</b>	Transmit the LLDP inventory TLV.
<b>location</b>	Transmit the LLDP location TLV.
<b>network-policy</b>	Transmit the LLDP network policy TLV.

### 2.24.3.1 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



### 2.24.4 lldp med all

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

**Format**            `lldp med all`  
**Mode**             Global Config

### 2.24.5 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

### 2.24.6 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

#### 2.24.6.1 no lldp med faststartrepeatcount

Use this command to return to the factory default value.

**Format**            `no lldp med faststartrepeatcount`  
**Mode**             Global Config

### 2.24.7 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

<b>Term</b>	<b>Definition</b>
<b>capabilities</b>	Transmit the LLDP capabilities TLV.
<b>ex-pd</b>	Transmit the LLDP extended PD TLV.
<b>ex-pse</b>	Transmit the LLDP extended PSE TLV.
<b>inventory</b>	Transmit the LLDP inventory TLV.
<b>location</b>	Transmit the LLDP location TLV.
<b>network-policy</b>	Transmit the LLDP network policy TLV.



### 2.24.7.1 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

### 2.24.8 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) #
```

### 2.24.9 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) #

```

### 2.24.10 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

```

### 2.24.11 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

```

### 2.24.12 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
```

## 2.25 Denial of Service Commands

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 six types of attacks:

- **SIP=DIP:** Source IP address = Destination IP address.



- **First Fragment:** TCP Header size smaller than configured value.
- **TCP Fragment:** IP Fragment Offset = 1.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.

### 2.25.1 dos-control all

This command enables Denial of Service protection checks globally.

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

#### 2.25.1.1 no dos-control all

This command disables Denial of Service prevention checks globally.

**Format** `no dos-control all`  
**Mode** Global Config

### 2.25.2 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

#### 2.25.2.1 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

### 2.25.3 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 than 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



### 2.25.3.1 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

### 2.25.4 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

### 2.25.4.1 no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

**Format** no dos-control tcpfrag

**Mode** Global Config

### 2.25.5 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

### 2.25.5.1 no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

**Format** no dos-control tcpflag

**Mode** Global Config



## 2.25.6 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

### 2.25.6.1 no dos-control l4port

This command disables L4 Port Denial of Service protections.

**Format** `no dos-control l4port`  
**Mode** Global Config

## 2.25.7 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

### 2.25.7.1 no dos-control icmp

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

**Format** `no dos-control icmp`  
**Mode** Global Config

## 2.25.8 show dos-control

This command displays Denial of Service configuration information.

**Format** `show dos-control`  
**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>SIPDIP Mode</b>	May be enabled or disabled. The factory default is disabled.
<b>First Fragment Mode</b>	May be enabled or disabled. The factory default is disabled.



<i>Term</i>	<i>Definition</i>
<b>Min TCP Hdr Size</b> <0-255>	The factory default is 20.
<b>TCP Fragment Mode</b>	May be enabled or disabled. The factory default is disabled.
<b>TCP Flag Mode</b>	May be enabled or disabled. The factory default is disabled.
<b>L4 Port Mode</b>	May be enabled or disabled. The factory default is disabled.
<b>ICMP Mode</b>	May be enabled or disabled. The factory default is disabled.
<b>Max ICMP Pkt Size</b> <0-1023>	The factory default is 512.

## 2.26 MAC Database Commands

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

### 2.26.1 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.

<b>Default</b>	300
<b>Format</b>	<code>bridge aging-time &lt;10-1,000,000&gt;</code>
<b>Mode</b>	Global Config

#### 2.26.1.1 no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

<b>Format</b>	<code>no bridge aging-time</code>
<b>Mode</b>	Global Config

### 2.26.2 show forwardingdb agetime

This command displays the timeout for address aging. In an IVL system, the *[fdbid | all]* parameter is required.

<b>Default</b>	all
<b>Format</b>	<code>show forwardingdb agetime [fdbid   all]</code>
<b>Mode</b>	Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Forwarding DB ID</b>	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.
<b>AgeTime</b>	<ul style="list-style-type: none"> <li>In an IVL system, this parameter displays the address aging timeout for the associated forwarding database.</li> <li></li> </ul>



### 2.26.3 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

<b>Term</b>	<b>Definition</b>
<b>MAC Address</b>	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.
<b>Type</b>	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.
<b>Component</b>	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
<b>Description</b>	The text description of this multicast table entry.
<b>Interfaces</b>	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
<b>Forwarding Interfaces</b>	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.

### 2.26.4 show mac-address-table stats

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

**Format**            `show mac-address-table stats`  
**Mode**             Privileged EXEC

<b>Term</b>	<b>Definition</b>
<b>Total Entries</b>	The total number of entries that can possibly be in the Multicast Forwarding Database table.
<b>Most MFDB Entries Ever Used</b>	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.
<b>Current Entries</b>	The current number of entries in the MFDB.

## 2.27 ISDP Commands

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

### 2.27.1 isdp run

This command enables ISDP on the switch.

**Default**            Enabled  
**Format**            `isdp run`  
**Mode**             Global Config



### 2.27.1.1 no isdp run

This command disables ISDP on the switch.

**Format** no isdp run

**Mode** Global Config

### 2.27.2 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

### 2.27.3 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

### 2.27.4 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

#### 2.27.4.1 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

### 2.27.5 isdp enable

This command enables ISDP on the interface.

**Default** Enabled

**Format** isdp enable

**Mode** Interface Config





### 2.27.5.1 no isdp enable

This command disables ISDP on the interface.

**Format**            `no isdp enable`  
**Mode**             Interface Config

### 2.27.6 clear isdp counters

This command clears ISDP counters.

**Format**            `clear isdp counters`  
**Mode**             Privileged EXEC

### 2.27.7 clear isdp table

This command clears entries in the ISDP table.

**Format**            `clear isdp table`  
**Mode**             Privileged EXEC

### 2.27.8 show isdp

This command displays global ISDP settings.

**Format**            `show isdp`  
**Mode**             Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Timer</b>	The frequency with which this device sends ISDP packets. This value is given in seconds.
<b>Hold Time</b>	The length of time the receiving device should save information sent by this device. This value is given in seconds.
<b>ISDPv2 Advertisements</b>	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
<b>Device ID</b>	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
<b>Device ID Format Capability</b>	Indicates the Device ID format capability of the device. <ul style="list-style-type: none"> <li><code>serialNumber</code> indicates that the device uses a serial number as the format for its Device ID.</li> <li><code>macAddress</code> indicates that the device uses a Layer 2 MAC address as the format for its Device ID.</li> <li><code>other</code> indicates that the device uses its platform-specific format as the format for its Device ID.</li> </ul>
<b>Device ID Format</b>	Indicates the Device ID format of the device. <ul style="list-style-type: none"> <li><code>serialNumber</code> indicates that the value is in the form of an ASCII string containing the device serial number.</li> <li><code>macAddress</code> indicates that the value is in the form of a Layer 2 MAC address.</li> <li><code>other</code> 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.</li> </ul>



### 2.27.9 show isdp interface

This command displays ISDP settings for the specified interface.

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

**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Mode</b>	ISDP mode enabled/disabled status for the interface(s).

### 2.27.10 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

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

### 2.27.11 show isdp neighbors

This command displays the list of neighboring devices.

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

**Mode** Privileged EXEC



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

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

```
(Broadcom 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
```

## 2.27.12 show isdp traffic

This command displays ISDP statistics.

**Format**        `show isdp traffic`  
**Mode**         Privileged EXEC

<b>Term</b>	<b>Definition</b>
<b>ISDP Packets Received</b>	Total number of ISDP packets received
<b>ISDP Packets Transmitted</b>	Total number of ISDP packets transmitted



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

### 2.27.13 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

#### 2.27.13.1 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

## 2.28 Multicast Handling Commands

### 2.28.1 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`  
**Mode** Interface Config

### 2.28.2 show port multicast

This command displays the port based multicast handling. The command 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`

**Mode** Privileged Exec

### 2.28.3 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 1-4094. If a created VLAN is deleted again, the flooding mode is reset to default.

**Format** `multicast`

**Mode** VLAN Config

### 2.28.4 show vlan multicast

This command displays the VLAN based multicast handling. The command displays for a specified VLAN ID (range is 1-4094) 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`

**Mode** Privileged Exec

### 2.28.5 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

#### 2.28.5.1 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



## 2.29 Port Bridging Commands

### 2.29.1 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

#### 2.29.1.1 no L2-port-bridge

This command resets L2 port bridging..

**Format** `no L2-port-bridge`

**Mode** Interface Config



---

*Chapter* **3**

---

---

# Quality of Service Commands

---



## 3. Quality of Service (QoS) 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 (CoS) Commands” on page 3 - 2
- 3.2 “Differentiated Services (DiffServ) Commands” on page 3 - 8
- 3.3 “DiffServ Class Commands” on page 3 - 9
- 3.4 “DiffServ Policy Commands” on page 3 - 17
- 3.5 “DiffServ Service Commands” on page 3 - 21
- 3.6 “DiffServ Show Commands” on page 3 - 22
- 3.7 “MAC Access Control List (ACL) Commands” on page 3 - 26
- 3.8 “IP Access Control List (ACL) Commands” on page 3 - 30
- 3.9 “IPv6 Access Control List (ACL) Commands” on page 3 - 35
- 3.10 “Auto-Voice over IP Commands” on page 3 - 38



**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 (CoS) Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.



**Note:** Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

#### 3.1.1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The *<userpriority>* values can range from 0-7. The *<trafficclass>* values range from 0-6, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see 2.5 “Voice VLAN Commands” on page 2 - 32.

**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 - 32.

**Format**            `show classofservice dot1p-mapping [<slot/port>]`  
**Mode**              Privileged EXEC

The following information is repeated for each user priority.

<i>Term</i>	<i>Definition</i>
<b>User Priority</b>	The 802.1p user priority value.
<b>Traffic Class</b>	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.

<i>Term</i>	<i>Definition</i>
<b>IP Precedence</b>	The IP Precedence value.
<b>Traffic Class</b>	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.

<i>Term</i>	<i>Definition</i>
<b>IP DSCP</b>	The IP DSCP value.
<b>Traffic Class</b>	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



<i>Term</i>	<i>Definition</i>
<b>Non-IP Traffic Class</b>	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).
<b>Untrusted Traffic Class</b>	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

<i>Term</i>	<i>Definition</i>
<b>Queue Id</b>	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
<b>Minimum Bandwidth</b>	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.
<b>Scheduler Type</b>	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
<b>Queue Management Type</b>	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
<b>Interface Shaping Rate</b>	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 interface cos-counter

This command displays the number of COS dropped packets. The counter is incremented if packets are dropped because of COS on egress side. The counter is shown for the specified interface. Note, that this counter can't be cleared on the hardware.

**Format**            `show interface cos-counter <slot/port>`  
**Mode**             Privileged EXEC

### 3.1.13 show packet-memory

This command displays the packet-memory limits. It displays some general values (the number of existing COS queues and the number of available cells) and a table of the configured limits for all interfaces. The configured limits consist of static cell limits for each COS queue, dynamic cell limit and low water mark. The cell limits are listed in



absolute cell count or percent of the available cells (1/1000 percent). The low water mark is a number (0.75%, 1.50%, 2.25%, 3.12,5%).

**Format**            `show packet-memory {cells|percent}`  
**Mode**              Privileged EXEC

### 3.1.14            packet-memory (configure)

This command configures the packet-memory limits for all ports or the CPU port. The static limits must be set for all COS queues (see 'show packet-memory') separated by comma. If configuring the packet-memory you **should** know exactly what to do. No checks for the limits are done except that the maximal memory value is not exceeded for each single limit. Therefore the user can configure step by step all information even if the sum of the static limits exceeds the packet memory temporarily. To activate the configuration it must be saved (normal saving) and a reset must be executed. Before saving it is checked that the sum of all static limits don't exceed the maximal memory. The dynamic cells may exceed this limit.

**Format**            `packet-memory {all|cpu} {cells|percent} <static-limits> <dynamic-limit>`  
`packet-memory {all|cpu} lwm <value>`  
**Mode**              Global Config

### 3.1.15            packet-memory (interface)

This command configures the packet-memory limits for the related interface. See detailed under 'packet-memory' above.

**Format**            `packet-memory {cells|percent} <static-limits> <dynamic-limit>`  
`packet-memory lwm <value>`  
**Mode**              Interface Config

### 3.1.16            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..3>`  
`show protection-group all`  
`show protection-group mask <slot/port>`  
`show protection-group mask all`  
**Mode**              Privileged EXEC

### 3.1.17            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..3>`  
`protection-group <0..3> name <name>`  
**Mode**              Global Config



### 3.1.17.1 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..3>`  
                      `no protection-group <0..3> name <name>`

**Mode**              Global Config

### 3.1.18 protection-group (interface)

This command is used to add an interface to a protection group. Each interface must be member of only one protection group. If a port is member in a protection group it may sent packets to ports which are not member of any group and to ports in the same group, but not to ports in another group.

**Format**            `protection-group <0..3>`

**Mode**              Interface Config

#### 3.1.18.1 no protection-group (interface)

This command is used to delete an interface from a protection group.

**Format**            `no protection-group <0..3>`

**Mode**              Interface Config

## 3.2 Differentiated Services (DiffServ) Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
  - 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 reffclass 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

### 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.

<b>Default</b>	none
<b>Format</b>	<b>match destination-address mac</b> <macaddr> <macmask>
<b>Mode</b>	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.

<b>Default</b>	none
<b>Format</b>	<b>match dstip</b> <ipaddr> <ipmask>
<b>Mode</b>	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.

<b>Default</b>	none
<b>Format</b>	<b>match dstip6</b> <destination-ipv6-prefix/prefix-length>
<b>Mode</b>	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.

<b>Default</b>	none
<b>Format</b>	<b>match dstl4port</b> {<portkey>   <0-65535>}
<b>Mode</b>	Ipv6-Class-Map Config 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** Ipv6-Class-Map Config  
 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.

<b>Default</b>	none
<b>Format</b>	<b>match protocol</b> { <i>&lt;protocol-name&gt;</i>   <i>&lt;0-255&gt;</i> }
<b>Mode</b>	Ipv6-Class-Map Config 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.

<b>Default</b>	none
<b>Format</b>	<b>match source-address mac</b> <i>&lt;address&gt;</i> <i>&lt;macmask&gt;</i>
<b>Mode</b>	Ipv6-Class-Map Config 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.

<b>Default</b>	none
<b>Format</b>	<b>match srcip</b> <i>&lt;ipaddr&gt;</i> <i>&lt;ipmask&gt;</i>
<b>Mode</b>	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.

<b>Default</b>	none
<b>Format</b>	<code>match srcip6 &lt;source-ipv6-prefix/prefix-length&gt;</code>
<b>Mode</b>	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.

<b>Default</b>	none
<b>Format</b>	<code>match srcl4port {&lt;portkey&gt;   &lt;0-65535&gt;}</code>
<b>Mode</b>	Ipv6-Class-Map Config 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.

<b>Default</b>	none
<b>Format</b>	<code>match vlan &lt;1-4095&gt;</code>
<b>Mode</b>	Ipv6-Class-Map Config 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.

<b>Default</b>	none
----------------	------



<b>Format</b>	<code>match secondary-vlan &lt;1-4095&gt;</code>
<b>Mode</b>	Ipv6-Class-Map Config 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.

<b>Format</b>	<code>assign-queue &lt;queueid&gt;</code>
<b>Mode</b>	Policy-Class-Map Config
<b>Incompatibilities</b>	Drop

#### 3.4.2 drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

<b>Format</b>	<code>drop</code>
<b>Mode</b>	Policy-Class-Map Config
<b>Incompatibilities</b>	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 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. `mark ip-dscp`

**Default**            1  
**Format**            `mark-cos <0-7>`  
**Mode**             Policy-Class-Map Config  
**Incompatibilities** Drop, Mark IP DSCP, IP Precedence, Police

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

### 3.4.8 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



### 3.4.9 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)

### 3.4.10 policy-map

This command establishes a new DiffServ policy. The *<polycyname>* 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 <polycyname> in`

**Mode** Global Config

#### 3.4.10.1 no policy-map

This command eliminates an existing DiffServ policy. The *<polycyname>* 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 <polycyname>`

**Mode** Global Config



### 3.4.11 policy-map rename

This command changes the name of a DiffServ policy. The *<polycyname>* is the name of an existing DiffServ class. The *<newpolycyname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

**Format**            `policy-map rename <polycyname> <newpolycyname>`  
**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 *<polycyname>* 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 <polycyname>`  
**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 *<polycyname>* 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 <policy-mapname>`

- 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:

<b>Term</b>	<b>Definition</b>
<b>Class Name</b>	The name of this class.
<b>Class Type</b>	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.
<b>L3 Proto</b>	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
<b>Match Criteria</b>	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.
<b>Values</b>	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:

<b>Term</b>	<b>Definition</b>
<b>Class Name</b>	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.)
<b>Class Type</b>	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.
<b>Ref Class Name</b>	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

<i>Term</i>	<i>Definition</i>
<b>DiffServ Admin mode</b>	The current value of the DiffServ administrative mode.
<b>Class Table Size</b>	The current number of entries (rows) in the Class Table.
<b>Class Table Max</b>	The maximum allowed entries (rows) for the Class Table.
<b>Class Rule Table Size</b>	The current number of entries (rows) in the Class Rule Table.
<b>Class Rule Table Max</b>	The maximum allowed entries (rows) for the Class Rule Table.
<b>Policy Table Size</b>	The current number of entries (rows) in the Policy Table.
<b>Policy Table Max</b>	The maximum allowed entries (rows) for the Policy Table.
<b>Policy Instance Table Size</b>	Current number of entries (rows) in the Policy Instance Table.
<b>Policy Instance Table Max</b>	Maximum allowed entries (rows) for the Policy Instance Table.
<b>Policy Attribute Table Size</b>	Current number of entries (rows) in the Policy Attribute Table.
<b>Policy Attribute Table Max</b>	Maximum allowed entries (rows) for the Policy Attribute Table.
<b>Service Table Size</b>	The current number of entries (rows) in the Service Table.
<b>Service Table Max</b>	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:

<i>Term</i>	<i>Definition</i>
<b>Policy Name</b>	The name of this policy.
<b>Type</b>	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):

<b>Term</b>	<b>Definition</b>
<b>Assign Queue</b>	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.
<b>Class Name</b>	The name of this class.
<b>Committed Burst Size (KB)</b>	The committed burst size, used in simple policing.
<b>Committed Rate (Kbps)</b>	The committed rate, used in simple policing.
<b>Conform Action</b>	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.
<b>Conform COS</b>	The CoS mark value if the conform action is set-cos-transmit.
<b>Conform DSCP Value</b>	The DSCP mark value if the conform action is set-dscp-transmit.
<b>Conform IP Precedence Value</b>	The IP Precedence mark value if the conform action is set-prec-transmit.
<b>Drop</b>	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.
<b>Mark CoS</b>	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.
<b>Mark IP DSCP</b>	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.
<b>Mark IP Precedence</b>	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.
<b>Mirror</b>	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.
<b>Non-Conform Action</b>	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.
<b>Non-Conform COS</b>	The CoS mark value if the non-conform action is set-cos-transmit.
<b>Non-Conform DSCP Value</b>	The DSCP mark value if the non-conform action is set-dscp-transmit.
<b>Non-Conform IP Precedence Value</b>	The IP Precedence mark value if the non-conform action is set-prec-transmit.
<b>Policing Style</b>	The style of policing, if any, used (simple).
<b>Redirect</b>	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:

<b>Term</b>	<b>Definition</b>
<b>Policy Name</b>	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
<b>Policy Type</b>	The policy type (Only inbound is supported).
<b>Class Members</b>	List of all class names associated with this policy.



### 3.6.4 show diffserv service

This command displays policy service information for the specified interface and direction. The *<slot/port>* parameter specifies a valid slot/port number for the system.

**Format**            `show diffserv service <slot/port> in`

**Mode**             Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>DiffServ Admin Mode</b>	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.
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Direction</b>	The traffic direction of this interface service.
<b>Operational Status</b>	The current operational status of this DiffServ service interface.
<b>Policy Name</b>	The name of the policy attached to the interface in the indicated direction.
<b>Policy Details</b>	Attached policy details, whose content is identical to that described for the show policy-map <i>&lt;polycymapname&gt;</i> 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

<i>Term</i>	<i>Definition</i>
<b>DiffServ Mode</b>	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):

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Direction</b>	The traffic direction of this interface service.
<b>OperStatus</b>	The current operational status of this DiffServ service interface.
<b>Policy Name</b>	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

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Direction</b>	The traffic direction of this interface service.
<b>Operational Status</b>	The current operational status of this DiffServ service interface.
<b>Policy Name</b>	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:

<i>Term</i>	<i>Definition</i>
<b>Class Name</b>	The name of this class instance.
<b>In Discarded Packets</b>	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):

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	Valid slot and port number separated by a forward slash.
<b>Operational Status</b>	The current operational status of this DiffServ service interface.
<b>Policy Name</b>	The name of the policy attached to the interface.
<b>Note:</b>	

## 3.7 MAC Access Control List (ACL) Commands

This section describes the commands you use to configure MAC ACL settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you 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**

<b>Ethertype Keyword</b>	<b>Corresponding Value</b>
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.

**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

<b>Term</b>	<b>Definition</b>
<b>Rule Number</b>	The ordered rule number identifier defined within the MAC ACL.
<b>Action</b>	The action associated with each rule. The possible values are Permit or Deny.
<b>Source MAC Address</b>	The source MAC address for this rule.
<b>Destination MAC Address</b>	The destination MAC address for this rule.
<b>Ethertype</b>	The Ethertype keyword or custom value for this rule.
<b>VLAN ID</b>	The VLAN identifier value or range for this rule.
<b>COS</b>	The COS (802.1p) value for this rule.
<b>Log</b>	Displays when you enable logging for the rule.



<i>Term</i>	<i>Definition</i>
<b>Assign Queue</b>	The queue identifier to which packets matching this rule are assigned.
<b>Mirror Interface</b>	On Broadcom 5650x platforms, the slot/port to which packets matching this rule are copied.
<b>Redirect Interface</b>	On Broadcom 5650x platforms, the slot/port to which packets matching this rule are forwarded.

## 3.8 IP Access Control List (ACL) Commands

This section describes the commands you use to configure IP ACL settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- FASTPATH software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is 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
<code>&lt;1-99&gt; or &lt;100-199&gt;</code>	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.
<code>{deny   permit}</code>	Specifies whether the IP ACL rule permits or denies an action. <b>Note:</b> For 5630x and 5650x-based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.
<code>every</code>	Match every packet
<code>{icmp   igmp   ip   tcp   udp   &lt;number&gt;}</code>	Specifies the protocol to filter for an extended IP ACL rule.
<code>&lt;srcip&gt; &lt;srcmask&gt;</code>	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
<code>[{eq {&lt;portkey&gt;   &lt;0-65535&gt;}}]</code>	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 <code>&lt;portkey&gt;</code> , which can be one of the following keywords: <code>domain</code> , <code>echo</code> , <code>ftp</code> , <code>ftpdata</code> , <code>http</code> , <code>smtp</code> , <code>snmp</code> , <code>telnet</code> , <code>tftp</code> , and <code>www</code> . Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
<code>&lt;dstip&gt; &lt;dstmask&gt;</code>	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
<code>[precedence &lt;precedence&gt;   tos &lt;tos&gt; &lt;tosmask&gt;   dscp &lt;dscp&gt;]</code>	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters <code>dscp</code> , <code>precedence</code> , <code>tos/tosmask</code> .
<code>[log]</code>	Specifies that this rule is to be logged.
<code>[assign-queue &lt;queue-id&gt;]</code>	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
<code>[{mirror   redirect} &lt;slot/port&gt;]</code>	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 <code>mirror</code> and <code>redirect</code> 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 <newname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails if an IP ACL by the name <newname> 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.



<b>Format</b>	<code>{deny   permit} {every   {{icmp   igmp   ip   tcp   udp   &lt;number&gt;}} &lt;srcip&gt; &lt;srcmask&gt; [{eq {&lt;portkey&gt;   &lt;0-65535&gt;}} &lt;dstip&gt; &lt;dstmask&gt; [{eq {&lt;portkey&gt;   &lt;0-65535&gt;}}] [precedence &lt;precedence&gt;   tos &lt;tos&gt; &lt;tosmask&gt;   dscp &lt;dscp&gt;] [log] [assign-queue &lt;queue-id&gt;] [{mirror   redirect} &lt;unit/slot/port&gt;]}</code>
<b>Mode</b>	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.

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.

<b>Default</b>	none
<b>Format</b>	<code>ip access-group &lt;accesslistnumber&gt; [vlan &lt;vlan-id&gt;] in [sequence &lt;1-4294967295&gt;]</code>
<b>Modes</b>	<ul style="list-style-type: none"> <li>• Interface Config</li> <li>• Global Config</li> </ul>

#### 3.8.5.1 no ip access-group

This command removes a specified IP ACL from an interface.

<b>Default</b>	none
<b>Format</b>	<code>no ip access-group &lt;accesslistnumber&gt; [vlan &lt;vlan-id&gt;] in</code>
<b>Mode</b>	<ul style="list-style-type: none"> <li>• Interface Config</li> <li>• Global Config</li> </ul>

### 3.8.6 acl-trapflags

This command enables the ACL trap mode.

<b>Default</b>	disabled
<b>Format</b>	<code>acl-trapflags</code>
<b>Mode</b>	Global Config

#### 3.8.6.1 no acl-trapflags

This command disables the ACL trap mode.

<b>Format</b>	<code>no acl-trapflags</code>
<b>Mode</b>	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.

<b>Term</b>	<b>Definition</b>
<b>Rule Number</b>	The number identifier for each rule that is defined for the IP ACL.
<b>Action</b>	The action associated with each rule. The possible values are Permit or Deny.
<b>Match All</b>	Indicates whether this access list applies to every packet. Possible values are True or False.
<b>Protocol</b>	The protocol to filter for this rule.
<b>Source IP Address</b>	The source IP address for this rule.
<b>Source IP Mask</b>	The source IP Mask for this rule.
<b>Source L4 Port Keyword</b>	The source port for this rule.
<b>Destination IP Address</b>	The destination IP address for this rule.





<b>Term</b>	<b>Definition</b>
<b>Destination IP Mask</b>	The destination IP Mask for this rule.
<b>Destination L4 Port Keyword</b>	The destination port for this rule.
<b>IP DSCP</b>	The value specified for IP DSCP.
<b>IP Precedence</b>	The value specified IP Precedence.
<b>IP TOS</b>	The value specified for IP TOS.
<b>Log</b>	Displays when you enable logging for the rule.
<b>Assign Queue</b>	The queue identifier to which packets matching this rule are assigned.
<b>Mirror Interface</b>	The slot/port to which packets matching this rule are copied.
<b>Redirect Interface</b>	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

<b>Term</b>	<b>Definition</b>
<b>ACL Type</b>	Type of access list (IP, IPv6, or MAC).
<b>ACL ID</b>	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
<b>Sequence Number</b>	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 (ACL) Commands

This section describes the commands you use to configure IPv6 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 if 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 specified IPv6 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.

**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



<i>Term</i>	<i>Definition</i>
<b>Rule Number</b>	The ordered rule number identifier defined within the IPv6 ACL.
<b>Action</b>	The action associated with each rule. The possible values are Permit or Deny.
<b>Match All</b>	Indicates whether this access list applies to every packet. Possible values are True or False.
<b>Protocol</b>	The protocol to filter for this rule.
<b>Source IP Address</b>	The source IP address for this rule.
<b>Source L4 Port Keyword</b>	The source port for this rule.
<b>Destination IP Address</b>	The destination IP address for this rule.
<b>Destination L4 Port Keyword</b>	The destination port for this rule.
<b>IP DSCP</b>	The value specified for IP DSCP.
<b>Flow Label</b>	The value specified for IPv6 Flow Label.
<b>Log</b>	Displays when you enable logging for the rule.
<b>Assign Queue</b>	The queue identifier to which packets matching this rule are assigned.
<b>Mirror Interface</b>	The slot/port to which packets matching this rule are copied.
<b>Redirect Interface</b>	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.

<b>Default</b>	disabled
<b>Format</b>	<code>auto-voip all</code>
<b>Mode</b>	Global Config

##### 3.10.1.1 no auto-voip all

Use this command to disable VoIP Profile on the interfaces of the switch.

<b>Format</b>	<code>no auto-voip all</code>
<b>Mode</b>	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

<i>Field</i>	<i>Description</i>
<b>AutoVoIP Mode</b>	The Auto VoIP mode on the interface.
<b>Traffic Class</b>	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.





---

*Chapter* **4**

---

---

# Utility Commands

---



## 4. Utility Commands

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

The Utility Commands chapter includes the following sections:

- 4.1 “Commands for update and startup Configuration” on page 4 - 2
- 4.2 “Dual Image Commands” on page 4 - 3
- 4.3 “ATCA commands” on page 4 - 3
- 4.4 “System Information and Statistics Commands” on page 4 - 5
- 4.5 “Logging Commands” on page 4 - 20
- 4.6 “System Utility and Clear Commands” on page 4 - 25
- 4.7 “Simple Network Time Protocol (SNTP) Commands” on page 4 - 32
- 4.8 “DHCP Server Commands” on page 4 - 35
- 4.9 “DHCP Filtering” on page 4 - 45
- 4.10 “DNS Client Commands” on page 4 - 46
- 4.11 “Serviceability Packet Tracing Commands” on page 4 - 50
- 4.12 “Cable Test Command” on page 4 - 58
- 4.13 “sFlow Commands” on page 4 - 59



**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.

### 4.1 Commands for update and startup Configuration

The following commands are implemented to manipulate the Software images and configurations of the AT8404.

#### 4.1.1 download ipmifw

This command updates the IPMI firmware using a HPM.1 firmware image. It downloads an IPMI firmware image from URL and flashes the IPMC. The command is also used for updates of AMC (see section below). If the flash process is interrupted or fails, the IPMC will automatically recover and use the previously installed image.

**Format**            `download ipmifw <url> <ipmc | amcb1 | amcb2 | amcb3 | amcb4 | rtm>`  
**Mode**              Privileged EXEC

#### 4.1.2 download amcipmifw

This command updates the IPMI firmware on an AMC with a Kontron OEM firmware image. For download a HPM.1 firmware image use command “download ipmifw” (see above). It downloads an IPMI firmware image from URL and flashes the MMC on the AMC with the new image. If the flash process is interrupted or fails, the MMC will automatically recover and use the previously installed image

**Format**            `download amcipmifw <url> <amcb1 | amcb2 | amcb3 | amcb4>`





**Mode** Privileged EXEC

## 4.2 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.

### 4.2.1 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

### 4.2.2 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

### 4.2.3 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

### 4.2.4 filedescr

This command associates a given text description with an image. Any existing description will be replaced.

**Format** `filedescr {image1 | image2} <text-description>`

**Mode** Privileged EXEC

## 4.3 ATCA commands

### 4.3.1 set board sensor threshold

This command sets a new threshold value for a sensor. The <record-id> (of SDR) for a specific sensor is displayed by the related "show" command

**Format** `set board sensor threshold <record-id> <value-type> <value>`

**Mode** Privileged EXEC



Value-types are:

<b>Value-type</b>	<b>Description</b>
<b>lower-non-critical</b>	Set lower non-critical threshold value
<b>lower-critical</b>	Set lower critical threshold value
<b>lower-non-recover</b>	Set lower non-recoverable threshold value
<b>upper-non-critical</b>	Set upper non-critical threshold value
<b>upper-critical</b>	Set upper critical threshold value
<b>upper-non-recover</b>	Set upper non-recoverable threshold value

### 4.3.2 set board device-id

This command sets the device ID for the board. The device ID is used in the management device locator sensor (show boardinfo sensors).

**Format**            **set board device-id** *<string>*  
**Mode**             Privileged EXEC

### 4.3.3 show atca ekeying

This command displays the current ekeying status together with admin mode and link status for all interfaces

**Format**            **show atca ekeying all**  
**Mode**             Privileged EXEC

### 4.3.4 ekeying (interface)

This command enables the ekeying for one port. Default is enabled.

**Format**            **ekeying**  
**Mode**             Interface Config

#### 4.3.4.1 no ekeying (interface)

This command disables the ekeying for one port. Default is enabled.

**Format**            **no ekeying**  
**Mode**             Interface Config

### 4.3.5 ekeying all (configure)

This command enables the ekeying for all ports for which ekeying is possible. Default is enabled.

**Format**            **ekeying all**  
**Mode**             Global Config



#### 4.3.5.1 no ekeying all (configure)

This command disables the ekeying for all ports for which ekeying is possible.

**Format**            `no ekeying all`

**Mode**             Global Config

## 4.4 System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

### 4.4.1 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

<i>Term</i>	<i>Definition</i>
<b>IP Address</b>	IP address of the management interface or another device on the management network.
<b>MAC Address</b>	Hardware MAC address of that device.
<b>Interface</b>	For a service port the output is <i>Management</i> . For a network port, the output is the slot/port of the physical interface.

### 4.4.2 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

<i>Term</i>	<i>Definition</i>
<b>File</b>	The file in which the event originated.
<b>Line</b>	The line number of the event.
<b>Task Id</b>	The task ID of the event.
<b>Code</b>	The event code.
<b>Time</b>	The time this event occurred.



**Note:** Event log information is retained across a switch reset.



### 4.4.3 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 4.4.4 “show version” on page 4 - 6.

**Format** `show hardware`

**Mode** Privileged EXEC

### 4.4.4 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

<b>Term</b>	<b>Definition</b>
<b>Switch Description</b>	Text used to identify the product name of this switch.
<b>Machine Type</b>	The machine model as defined by the Vital Product Data.
<b>Machine Model</b>	The machine model as defined by the Vital Product Data
<b>Serial Number</b>	The unique box serial number for this switch.
<b>FRU Number</b>	The field replaceable unit number.
<b>Part Number</b>	Manufacturing part number.
<b>Maintenance Level</b>	Hardware changes that are significant to software.
<b>Manufacturer</b>	Manufacturer descriptor field.
<b>Burned in MAC Address</b>	Universally assigned network address.
<b>Software Version</b>	The release.version.revision number of the code currently running on the switch.
<b>Operating System</b>	The operating system currently running on the switch.
<b>Network Processing Device</b>	The type of the processor microcode.
<b>Additional Packages</b>	The additional packages incorporated into this system.

### 4.4.5 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:

<b>Parameters</b>	<b>Definition</b>
<b>Packets Received Without Error</b>	The total number of packets (including broadcast packets and multicast packets) received by the processor.
<b>Packets Received With Error</b>	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
<b>Broadcast Packets Received</b>	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
<b>Packets Transmitted Without Error</b>	The total number of packets transmitted out of the interface.
<b>Transmit Packets Errors</b>	The number of outbound packets that could not be transmitted because of errors.
<b>Collisions Frames</b>	The best estimate of the total number of collisions on this Ethernet segment.
<b>Time Since Counters Last Cleared</b>	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:

<b>Term</b>	<b>Definition</b>
<b>Broadcast Packets Received</b>	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
<b>Packets Received With Error</b>	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
<b>Packets Transmitted Without Error</b>	The total number of packets transmitted out of the interface.
<b>Broadcast Packets Transmitted</b>	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.
<b>Transmit Packet Errors</b>	The number of outbound packets that could not be transmitted because of errors.
<b>Address Entries Currently In Use</b>	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
<b>VLAN Entries Currently In Use</b>	The number of VLAN entries presently occupying the VLAN table.
<b>Time Since Counters Last Cleared</b>	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

#### 4.4.6 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
<b>Packets Received</b>	<ul style="list-style-type: none"> <li>• <b>Total Packets Received (Octets)</b> - 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.</li> <li>• <b>Packets Received 64 Octets</b> - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</li> <li>• <b>Packets Received 65–127 Octets</b> - 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).</li> <li>• <b>Packets Received 128–255 Octets</b> - 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).</li> <li>• <b>Packets Received 256–511 Octets</b> - 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).</li> <li>• <b>Packets Received 512–1023 Octets</b> - 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).</li> <li>• <b>Packets Received 1024–1518 Octets</b> - 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).</li> <li>• <b>Packets Received &gt; 1522 Octets</b> - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.</li> <li>• <b>Packets RX and TX 64 Octets</b> - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).</li> <li>• <b>Packets RX and TX 65–127 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 128–255 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 256–511 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 512–1023 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 1024–1518 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 1519–1522 Octets</b> - 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).</li> <li>• <b>Packets RX and TX 1523–2047 Octets</b> - 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.</li> <li>• <b>Packets RX and TX 2048–4095 Octets</b> - 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.</li> <li>• <b>Packets RX and TX 4096–9216 Octets</b> - 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.</li> </ul>



<i>Term</i>	<i>Definition</i>
<b>Packets Received Successfully</b>	<ul style="list-style-type: none"> <li>• <b>Total Packets Received Without Error</b> - The total number of packets received that were without errors.</li> <li>• <b>Unicast Packets Received</b> - The number of subnetwork-unicast packets delivered to a higher-layer protocol.</li> <li>• <b>Multicast Packets Received</b> - 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.</li> <li>• <b>Broadcast Packets Received</b> - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.</li> </ul>
<b>Packets Received with MAC Errors</b>	<ul style="list-style-type: none"> <li>• <b>Total</b> - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</li> <li>• <b>Jabbers Received</b> - 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.</li> <li>• <b>Fragments/Undersize Received</b> - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).</li> <li>• <b>Alignment Errors</b> - 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.</li> <li>• <b>Rx FCS Errors</b> - 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.</li> <li>• <b>Overruns</b> - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.</li> </ul>
<b>Received Packets Not Forwarded</b>	<ul style="list-style-type: none"> <li>• <b>Total</b> - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process</li> <li>• <b>Local Traffic Frames</b> - The total number of frames dropped in the forwarding process because the destination address was located off of this port.</li> <li>• <b>802.3x Pause Frames Received</b> - 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.</li> <li>• <b>Unacceptable Frame Type</b> - The number of frames discarded from this port due to being an unacceptable frame type.</li> <li>• <b>Multicast Tree Viable Discards</b> - The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.</li> <li>• <b>Reserved Address Discards</b> - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.</li> <li>• <b>Broadcast Storm Recovery</b> - The number of frames discarded that are destined for <code>FF:FF:FF:FF:FF:FF</code> when Broadcast Storm Recovery is enabled.</li> <li>• <b>CFI Discards</b> - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.</li> <li>• <b>Upstream Threshold</b> - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.</li> </ul>





<i>Term</i>	<i>Definition</i>
<b>Packets Transmitted Octets</b>	<ul style="list-style-type: none"> <li>• <b>Total Bytes</b> - 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. -----</li> <li>• <b>Packets Transmitted 64 Octets</b> - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</li> <li>• <b>Packets Transmitted 65-127 Octets</b> - 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).</li> <li>• <b>Packets Transmitted 128-255 Octets</b> - 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).</li> <li>• <b>Packets Transmitted 256-511 Octets</b> - 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).</li> <li>• <b>Packets Transmitted 512-1023 Octets</b> - 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).</li> <li>• <b>Packets Transmitted 1024-1518 Octets</b> - 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).</li> <li>• <b>Max Frame Size</b> - The maximum size of the Info (non-MAC) field that this port will receive or transmit.</li> </ul>
<b>Packets Transmitted Successfully</b>	<ul style="list-style-type: none"> <li>• <b>Total</b> - The number of frames that have been transmitted by this port to its segment.</li> <li>• <b>Unicast Packets Transmitted</b> - 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.</li> <li>• <b>Multicast Packets Transmitted</b> - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.</li> <li>• <b>Broadcast Packets Transmitted</b> - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.</li> </ul>
<b>Transmit Errors</b>	<ul style="list-style-type: none"> <li>• <b>Total Errors</b> - The sum of Single, Multiple, and Excessive Collisions.</li> <li>• <b>Tx FCS Errors</b> - 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.</li> <li>• <b>Oversized</b> - 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.</li> <li>• <b>Underrun Errors</b> - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.</li> </ul>
<b>Transmit Discards</b>	<ul style="list-style-type: none"> <li>• <b>Total Discards</b> - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.</li> <li>• <b>Single Collision Frames</b> - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</li> <li>• <b>Multiple Collision Frames</b> - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</li> <li>• <b>Excessive Collisions</b> - A count of frames for which transmission on a particular interface fails due to excessive collisions.</li> <li>• <b>Port Membership Discards</b> - The number of frames discarded on egress for this port due to egress filtering being enabled.</li> </ul>



<i>Term</i>	<i>Definition</i>
<b>Protocol Statistics</b>	<ul style="list-style-type: none"> <li>• <b>802.3x Pause Frames Transmitted</b> - 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.</li> <li>• <b>GVRP PDUs Received</b> - The count of GVRP PDUs received in the GARP layer.</li> <li>• <b>GVRP PDUs Transmitted</b> - The count of GVRP PDUs transmitted from the GARP layer.</li> <li>• <b>GVRP Failed Registrations</b> - The number of times attempted GVRP registrations could not be completed.</li> <li>• <b>GMRP PDUs Received</b> - The count of GMRP PDU's received in the GARP layer.</li> <li>• <b>GMRP PDUs Transmitted</b> - The count of GMRP PDU's transmitted from the GARP layer.</li> <li>• <b>GMRP Failed Registrations</b> - The number of times attempted GMRP registrations could not be completed.</li> <li>• <b>STP BPDUs Transmitted</b> - Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>• <b>STP BPDUs Received</b> - Spanning Tree Protocol Bridge Protocol Data Units received.</li> <li>• <b>RST BPDUs Transmitted</b> - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>• <b>RSTP BPDUs Received</b> - Rapid Spanning Tree Protocol Bridge Protocol Data Units received.</li> <li>• <b>MSTP BPDUs Transmitted</b> - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.</li> <li>• <b>MSTP BPDUs Received</b> - Multiple Spanning Tree Protocol Bridge Protocol Data Units received.</li> </ul>
<b>Dot1x Statistics</b>	<ul style="list-style-type: none"> <li>• <b>EAPOL Frames Received</b> - The number of valid EAPOL frames of any type that have been received by this authenticator.</li> <li>• <b>EAPOL Frames Transmitted</b> - The number of EAPOL frames of any type that have been transmitted by this authenticator.</li> </ul>
<b>Time Since Counters Last Cleared</b>	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.

<i>Term</i>	<i>Definition</i>
<b>Octets Received</b>	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
<b>Total Packets Received Without Error</b>	The total number of packets (including broadcast packets and multicast packets) received by the processor.
<b>Unicast Packets Received</b>	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
<b>Multicast Packets Received</b>	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.
<b>Broadcast Packets Received</b>	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
<b>Receive Packets Discarded</b>	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.
<b>Octets Transmitted</b>	The total number of octets transmitted out of the interface, including framing characters.
<b>Packets Transmitted without Errors</b>	The total number of packets transmitted out of the interface.
<b>Unicast Packets Transmitted</b>	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.



<b>Term</b>	<b>Definition</b>
<b>Multicast Packets Transmitted</b>	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
<b>Broadcast Packets Transmitted</b>	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
<b>Transmit Packets Discarded</b>	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.
<b>Most Address Entries Ever Used</b>	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
<b>Address Entries in Use</b>	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
<b>Maximum VLAN Entries</b>	The maximum number of Virtual LANs (VLANs) allowed on this switch.
<b>Most VLAN Entries Ever Used</b>	The largest number of VLANs that have been active on this switch since the last reboot.
<b>Static VLAN Entries</b>	The number of presently active VLAN entries on this switch that have been created statically.
<b>Dynamic VLAN Entries</b>	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
<b>VLAN Deletes</b>	The number of VLANs on this switch that have been created and then deleted since the last reboot.
<b>Time Since Counters Last Cleared</b>	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

#### 4.4.7 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.

<b>Term</b>	<b>Definition</b>
<b>Mac Address</b>	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.
<b>Interface</b>	The port through which this address was learned.
<b>Interface Index</b>	This object indicates the ifIndex of the interface table entry associated with this port.



Term	Definition
<b>Status</b>	<p>The status of this entry. The meanings of the values are:</p> <ul style="list-style-type: none"> <li>• <i>Static</i>—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be released.</li> <li>• <i>Learned</i>—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.</li> <li>• <i>Management</i>—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.</li> <li>• <i>Self</i>—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address).</li> <li>• <i>GMRP Learned</i>—The value of the corresponding was learned via GMRP and applies to Multicast.</li> <li>• <i>Other</i>—The value of the corresponding instance does not fall into one of the other categories.</li> </ul>

If you enter the `interface <slot/port>` parameter, in addition to the MAC Address and Status fields, the following field appears:

Term	Definition
<b>VLAN ID</b>	The VLAN on which the MAC address was learned.

The following information displays if you enter the `count` parameter:

Term	Definition
<b>Dynamic Address count</b>	Number of MAC addresses in the forwarding database that were automatically learned.
<b>Static Address (User-defined) count</b>	Number of MAC addresses in the forwarding database that were manually entered by a user.
<b>Total MAC Addresses in use</b>	Number of MAC addresses currently in the forwarding database.
<b>Total MAC Addresses available</b>	Number of MAC addresses the forwarding database can handle.

#### 4.4.8 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

#### 4.4.9 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

#### 4.4.10 show sysinfo

This command displays switch information.

**Format** `show sysinfo`  
**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Switch Description</b>	Text used to identify this switch.
<b>System Name</b>	Name used to identify the switch. The factory default is blank. To configure the system name, see 5.8.1 “snmp-server” on page 5 - 21.
<b>System Location</b>	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see 5.8.1 “snmp-server” on page 5 - 21.
<b>System Contact</b>	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see 5.8.1 “snmp-server” on page 5 - 21.
<b>System ObjectID</b>	The base object ID for the switch’s enterprise MIB.
<b>System Up Time</b>	The time in days, hours and minutes since the last switch reboot.
<b>MIBs Supported</b>	A list of MIBs supported by this agent.

#### 4.4.11 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 logging
- show event log
- show logging buffered
- show trap log
- show running config

**Format** `show tech-support`  
**Mode** Privileged EXEC

#### 4.4.12 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

#### 4.4.12.1 no terminal length

Use this command to set the terminal length to the default value.

#### 4.4.13 show terminal length

Use this command to display the value of the user-configured terminal length size.

**Format** `show terminal length`  
**Mode** Privileged EXEC

#### 4.4.14 show boardinfo post-status

This command displays the system power on self test status.

**Format** `show boardinfo post-status system`  
**Mode** Privileged EXEC

#### 4.4.15 show boardinfo sensors

This command displays the current sensor readings. It can either display a compressed list of all sensors or display full readings for a specified sensor. The <record-id> (of SDR) for a specific sensor is displayed in the compressed list

**Format** `show boardinfo sensors {<record-id> | brief}`  
**Mode** Privileged EXEC



**Note:** It might take a while to get an output of the “*show boardinfo sensors brief*” command

#### 4.4.16 show boardinfo event-log

This command displays the event log of the board management controller. It can either display a summary (“info”) or a list of all existing event-log records, a list with most recent records or a single record. The <record-id> (of SEL) is displayed in the list of records.

**Format** `show boardinfo event-log {info | list [last <nr-of-most-recent-entries> | <record-id>]}`  
**Mode** Privileged EXEC



**Note:** It might take a while to get an output of the “*show boardinfo event-log list*” command



#### 4.4.17 **show boardinfo update-status**

This command displays the status of the firmware update process for the IPMI controller.

**Format** `show boardinfo update-status`

**Mode** Privileged EXEC

#### 4.4.18 **show boardinfo version**

This command displays hardware and software revision information. This includes serial-numbers, software and hardware revisions as applicable.

**Format** `show boardinfo version`

**Mode** Privileged EXEC

Version information included

- 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
- 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

#### 4.4.19 **show boardinfo address**

This command displays the global address info of the board.

**Format** `show boardinfo address`

**Mode** Privileged EXEC

#### 4.4.20 **show boardinfo fru**

This command displays various FRU (field replaceable unit) related information.

**Format** `show boardinfo fru {product-info | board-info | multi-record | custom-area | all}`

**Mode** Privileged EXEC





#### 4.4.21 show boardinfo ipmidev

This command displays the IPMI device information. This consists of Firmware Revision, IPMI version, Manufacturer and Product ID.

**Format**            `show boardinfo ipmidev`  
**Mode**             Privileged EXEC

#### 4.4.22 show boardinfo amc connection

This command displays the connections to the AMC, to the CPU0-2 and to the RTM.

**Format**            `show boardinfo amc connection {all | amcb1 | amcb2 | amcb3 | amcb4 | rtm}`  
**Mode**             Privileged EXEC

#### 4.4.23 show boardinfo amc fru

This command displays various FRU (field replaceable unit) related information (or all FRU information) for a specified AMC, CPU0-2 and RTM.

**Format**            `show boardinfo amc fru {product-info|board-info|multi-record|custom-area|all} {all|amcb1|amcb2|amcb3|amcb4|rtm}`  
**Mode**             Privileged EXEC

#### 4.4.24 show boardinfo amc ipmidev

This command displays the IPMI device information for a specified AMC. This includes Firmware Revision, IPMI version, Manufacturer and Product ID.

**Format**            `show boardinfo amc ipmidev {all|amcb1|amcb2|amcb3|amcb4|rtm}`  
**Mode**             Privileged EXEC

#### 4.4.25 show boardinfo led

This command displays the LED status of the ATCA LED's.

**Format**            `show boardinfo led`  
**Mode**             Privileged EXEC

#### 4.4.26 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**             Privileged EXEC



#### 4.4.27 show boardinfo memory-usage

This command displays the memory usage. It shows malloc and kernel statistics.

**Format** show boardinfo memory-usage

**Mode** Privileged EXEC

### 4.5 Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

#### 4.5.1 logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

**Default** disabled; critical when enabled

**Format** logging buffered

**Mode** Global Config

##### 4.5.1.1 no logging buffered

This command disables logging to in-memory log.

**Format** no logging buffered

**Mode** Global Config

#### 4.5.2 logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

**Default** enabled

**Format** logging buffered wrap

**Mode** Privileged EXEC

##### 4.5.2.1 no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

**Format** no logging buffered wrap

**Mode** Privileged EXEC

#### 4.5.3 logging cli-command

This command enables the CLI command logging feature, which enables the FASTPATH software to log all CLI commands issued on the system.

**Default** enabled



**Format** logging cli-command  
**Mode** Global Config

#### 4.5.3.1 no logging cli-command

This command disables the CLI command Logging feature.

**Format** no logging cli-command  
**Mode** Global Config

### 4.5.4 logging console

This command enables logging to the console. You can specify the `<severitylevel>` value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

**Default** disabled; critical when enabled  
**Format** logging console [*severitylevel*]  
**Mode** Global Config

#### 4.5.4.1 no logging console

This command disables logging to the console.

**Format** no logging console  
**Mode** Global Config

### 4.5.5 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

### 4.5.6 logging host remove

This command disables logging to host. See 4.5.11 “show logging hosts” on page 4 - 23 for a list of host indexes.

**Format** logging host remove *<hostindex>*  
**Mode** Global Config



### 4.5.7 logging port

This command sets the local port number of the LOG client for logging messages. The *<portid>* can be in the range from 1 to 65535.

**Default** 514  
**Format** `logging port <portid>`  
**Mode** Global Config

#### 4.5.7.1 no logging port

This command resets the local logging port to the default.

**Format** `no logging port`  
**Mode** Global Config

### 4.5.8 logging syslog

This command enables syslog logging. The *<portid>* parameter is an integer with a range of 1-65535.

**Default** disabled  
**Format** `logging syslog [port <portid>]`  
**Mode** Global Config

#### 4.5.8.1 no logging syslog

This command disables syslog logging.

**Format** `no logging syslog`  
**Mode** Global Config

### 4.5.9 show logging

This command displays logging configuration information.

**Format** `show logging`  
**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Logging Client Local Port</b>	Port on the collector/relay to which syslog messages are sent.
<b>CLI Command Logging</b>	Shows whether CLI Command logging is enabled.
<b>Console Logging</b>	Shows whether console logging is enabled.
<b>Console Logging Severity Filter</b>	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
<b>Buffered Logging</b>	Shows whether buffered logging is enabled.
<b>Syslog Logging</b>	Shows whether syslog logging is enabled.



<i>Term</i>	<i>Definition</i>
<b>Log Messages Received</b>	Number of messages received by the log process. This includes messages that are dropped or ignored.
<b>Log Messages Dropped</b>	Number of messages that could not be processed due to error or lack of resources.
<b>Log Messages Relayed</b>	Number of messages sent to the collector/relay.

#### 4.5.10 **show logging buffered**

This command displays buffered logging (system startup and system operation logs).

**Format** `show logging buffered`

**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Buffered (In-Memory) Logging</b>	Shows whether the In-Memory log is enabled or disabled.
<b>Buffered Logging Wrapping Behavior</b>	The behavior of the In Memory log when faced with a log full situation.
<b>Buffered Log Count</b>	The count of valid entries in the buffered log.

#### 4.5.11 **show logging hosts**

This command displays all configured logging hosts.

**Format** `show logging hosts`

**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Host Index</b>	(Used for deleting hosts.)
<b>IP Address / Hostname</b>	IP address or hostname of the logging host.
<b>Severity Level</b>	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).
<b>Port</b>	The server port number, which is the port on the local host from which syslog messages are sent.
<b>Host Status</b>	The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

#### 4.5.12 **show logging traplogs**

This command displays SNMP trap events and statistics.

**Format** `show logging traplogs`

**Mode** Privileged EXEC



<i>Term</i>	<i>Definition</i>
<b>Number of Traps Since Last Reset</b>	The number of traps since the last boot.
<b>Trap Log Capacity</b>	The number of traps the system can retain.
<b>Number of Traps Since Log Last Viewed</b>	The number of new traps since the command was last executed.
<b>Log</b>	The log number.
<b>System Time Up</b>	How long the system had been running at the time the trap was sent.
<b>Trap</b>	The text of the trap message.

#### 4.5.13 clear board event-log

This command deletes all event-log records

**Format**            `clear board event-log`  
**Mode**             Privileged EXEC

#### 4.5.14 show logging backtrace

This command displays the backtrace file last created. A backtrace file is created when the application stops unexpectedly.

**Format**            `show logging backtrace`  
**Mode**             Privileged EXEC

#### 4.5.15 show logging errcounter

This command displays the trace of the error counters.

**Format**            `show logging errcounter`  
**Mode**             Privileged EXEC

#### 4.5.16 clear errcounter

This command clears the error counters trace.

**Format**            `clear errcounter`  
**Mode**             Privileged EXEC

#### 4.5.17 show logging persistent

This command displays the persistent logging.

**Format**            `show logging persistent`  
**Mode**             Privileged EXEC



## 4.6 System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

### 4.6.1 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.

<b>Default</b>	<ul style="list-style-type: none"> <li>• count: 3 probes</li> <li>• interval: 3 seconds</li> <li>• size: 0 bytes</li> <li>• port: 33434</li> <li>• maxTtl: 30 hops</li> <li>• maxFail: 5 probes</li> <li>• initTtl: 1 hop</li> <li>•</li> </ul>
<b>Format</b>	<pre>traceroute &lt;ipaddr hostname&gt; [initTtl &lt;initTtl&gt;] [maxTtl &lt;maxTtl&gt;] [maxFail &lt;maxFail&gt;] [interval &lt;interval&gt;] [count &lt;count&gt;] [port &lt;port&gt;] [size &lt;size&gt;]</pre>
<b>Mode</b>	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
<code>ipaddr hostname</code>	The <code>ipaddr</code> value should be a valid IP address. The <code>hostname</code> value should be a valid hostname.
<code>initTtl</code>	Use <code>initTtl</code> 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.
<code>maxTtl</code>	Use <code>maxTtl</code> to specify the maximum TTL. Range is 1 to 255.
<code>maxFail</code>	Use <code>maxFail</code> to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
<code>interval</code>	Use <code>interval</code> to specify the time between probes, in seconds. Range is 1 to 60 seconds.
<code>count</code>	Use the optional <code>count</code> parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
<code>port</code>	Use the optional <code>port</code> 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.
<code>size</code>	Use the optional <code>size</code> 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
```

## 4.6.2 clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter **y**, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

**Note:** The "clear config" command resets all configuration settings, also the custom settings, e.g. customer specific ethx settings. To maintain the custom settings use the "copy nvram:factory-all nvram:startup-all" command instead.

**Format**        `clear config`  
**Mode**         Privileged EXEC

## 4.6.3 clear counters

This command clears the statistics for a specified `<slot/port>`, for all the ports, or for the entire switch based upon the argument.

**Format**        `clear counters {<slot/port> | all}`  
**Mode**         Privileged EXEC

## 4.6.4 clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

**Format**        `clear igmpsnooping`  
**Mode**         Privileged EXEC

## 4.6.5 clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

**Format**        `clear pass`  
**Mode**         Privileged EXEC





#### 4.6.6 clear port-channel

This command clears all port-channels (LAGs).

**Format** clear port-channel

**Mode** Privileged EXEC

#### 4.6.7 clear traplog

This command clears the trap log.

**Format** clear traplog

**Mode** Privileged EXEC

#### 4.6.8 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

**Format** clear vlan

**Mode** Privileged EXEC

#### 4.6.9 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

#### 4.6.10 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

#### 4.6.11 logout

This command closes the current telnet connection or resets the current serial connection.



**Note:** Save configuration changes before logging out.

**Format** logout

**Modes**

- Privileged EXEC
- User EXEC



### 4.6.12 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.

<b>Default</b>	<ul style="list-style-type: none"> <li>The default count is 1.</li> <li>The default interval is 3 seconds.</li> <li>The default size is 0 bytes.</li> </ul>
<b>Format</b>	<code>ping &lt;ipaddress hostname&gt; [count &lt;count&gt;] [interval &lt;interval&gt;] [size &lt;size&gt;]</code>
<b>Modes</b>	<ul style="list-style-type: none"> <li>Privileged EXEC</li> <li>User EXEC</li> </ul>

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Description
<b>count</b>	Use the <b>count</b> parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the <i>&lt;ip-address&gt;</i> field. The range for <i>&lt;count&gt;</i> is 1 to 15 requests.
<b>interval</b>	Use the <b>interval</b> parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
<b>size</b>	Use the <b>size</b> 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
```

#### 4.6.13 quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

**Format**            `quit`  
**Modes**            • Privileged EXEC  
                     • User EXEC

#### 4.6.14 reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

**Format**            `reload`  
**Mode**             Privileged EXEC

#### 4.6.15 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**             Privileged EXEC

#### 4.6.16 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 or Xmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management.

**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 one of the following values:

```
{xmodem | tftp://<ipaddr|hostname>|<ip6address>/<filepath>/<filename>
| sftp|scp://<username>@<ipaddr>|<ip6address>|<filepath>|<filename>}
```



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
<code>nvrām:backup-config</code>	<code>nvrām:startup-config</code>	Copies the backup configuration to the startup configuration.
<code>nvrām:factory-settings</code>	<code>nvrām:current-settings</code>	Copies factory settings file to current settings file
<code>nvrām:factory-profile</code>	<code>nvrām:current-profile</code>	Copies factory profile file to current profile file
<code>nvrām:factory-config</code>	<code>nvrām:current-config</code>	Copies factory configuration file to current configuration file
<code>nvrām:factory-all</code>	<code>nvrām:startup-all</code>	Copies all factory settings as configuration to be used after reboot.
<code>nvrām:clibanner</code>	<code>&lt;url&gt;</code>	Copies the CLI banner to a server.
<code>nvrām:current-settings</code>	<code>&lt;url&gt;</code>	Contains configuration parameter
<code>nvrām:diag-report</code>	<code>&lt;url&gt;</code>	Copies diagnostics result file to a server
<code>nvrām:errorlog</code>	<code>&lt;url&gt;</code>	Copies the error log file to a server.
<code>nvrām:extra-profile</code>	<code>&lt;url&gt;</code>	Contains customer specific configuration files. This "tar.gz"-file will be unpacked in the "/"-directory
<code>nvrām:fastpath.cfg</code>	<code>&lt;url&gt;</code>	Uploads the binary config file to a server.
<code>nvrām:log</code>	<code>&lt;url&gt;</code>	Copies the log file to a server.
<code>nvrām:oslog</code>	<code>&lt;url&gt;</code>	Copies the OS system log file to a server
<code>nvrām:script</code> <code>&lt;scriptname&gt;</code>	<code>&lt;url&gt;</code>	Copies a specified configuration script file to a server.
<code>nvrām:settings</code>	<code>&lt;url&gt;</code>	Copies the file containing current settings to a server
<code>nvrām:startup-config</code>	<code>nvrām:backup-config</code>	Copies the startup configuration to the backup configuration.
<code>nvrām:startup-config</code>	<code>&lt;url&gt;</code>	Copies the startup configuration to a server.
<code>nvrām:traplog</code>	<code>&lt;url&gt;</code>	Copies the trap log file to a server.
<code>system:running-config</code>	<code>nvrām:startup-config</code>	Saves the running configuration to nvrām.
<code>nvrām:all-config</code>	<code>&lt;url&gt;</code>	Uploads all relevant config files.
<code>&lt;url&gt;</code>	<code>nvrām:clibanner</code>	Downloads the CLI banner to the system.
<code>&lt;url&gt;</code>	<code>pld</code>	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.
<code>&lt;url&gt;</code>	<code>nvrām:fastpath.cfg</code>	Downloads the binary config file to the system.

Table 1: Copy Parameters (Continued)

Source	Destination	Description
<url>	<i>nvr</i> am: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>	<i>nvr</i> am:sshkey-dsa	Downloads an SSH key file. For more information, see 5.4 “Secure Shell (SSH) Commands” on page 5 - 11.
<url>	<i>nvr</i> am:sshkey-rsa1	Downloads an SSH key file.
<url>	<i>nvr</i> am:sshkey-rsa2	Downloads an SSH key file.
<url>	<i>nvr</i> am:current- settings	Downloads the file containing current settings to the system
<url>	<i>nvr</i> am:extra-profile	Downloads the extra-profile “tar.gz” file to the system
<url>	<i>nvr</i> am:startup-config	Downloads the startup configuration file to the system.
<url>	<i>nvr</i> am:all-config	Downloads all relevant config files.
<url>	{image1   image2}	Download an image from the remote server to either image.
{image1   image2}	<url>	Upload either image to the remote server.
image1	image2	Copy image1 to image2.
image2	image1	Copy image2 to image1.

#### 4.6.17 delete nvr:extra-profile

This command deletes the extra profile.

**Format**            `delete nvr:extra-profile`  
**Mode**             Privileged EXEC

#### 4.6.18 set bootstopkey

This command sets the bootstop key. With this key the booting process can be stopped. The key name is “stop”. This is the default setting.

**Format**            `set bootstopkey`  
**Mode**             Privileged EXEC

##### 4.6.18.1 no set bootstopkey

This command resets the bootstop key. The boot process can not be interrupted.

**Format**            `no set bootstopkey`  
**Mode**             Privileged EXEC



## 4.7 Simple Network Time Protocol (SNTP) Commands

This section describes the commands you use to automatically configure the system time and date by using SNTP.

### 4.7.1 `sntp broadcast client poll-interval`

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where `<poll-interval>` can be a value from 6 to 16.

**Default** 6  
**Format** `sntp broadcast client poll-interval <poll-interval>`  
**Mode** Global Config

#### 4.7.1.1 `no sntp broadcast client poll-interval`

This command resets the poll interval for SNTP broadcast client back to the default value.

**Format** `no sntp broadcast client poll-interval`  
**Mode** Global Config

### 4.7.2 `sntp client mode`

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

**Default** disabled  
**Format** `sntp client mode [broadcast | unicast]`  
**Mode** Global Config

#### 4.7.2.1 `no sntp client mode`

This command disables Simple Network Time Protocol (SNTP) client mode.

**Format** `no sntp client mode`  
**Mode** Global Config

### 4.7.3 `sntp client port`

This command sets the SNTP client port id to a value from 1-65535.

**Default** 123  
**Format** `sntp client port <portid>`  
**Mode** Global Config

#### 4.7.3.1 `no sntp client port`

This command resets the SNTP client port back to its default value.

**Format** `no sntp client port`



**Mode** Global Config

#### 4.7.4 sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where `<poll-interval>` can be a value from 6 to 16.

**Default** 6

**Format** `sntp unicast client poll-interval <poll-interval>`

**Mode** Global Config

##### 4.7.4.1 no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

**Format** `no sntp unicast client poll-interval`

**Mode** Global Config

#### 4.7.5 sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

**Default** 5

**Format** `sntp unicast client poll-timeout <poll-timeout>`

**Mode** Global Config

##### 4.7.5.1 no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

**Format** `no sntp unicast client poll-timeout`

**Mode** Global Config

#### 4.7.6 sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

**Default** 1

**Format** `sntp unicast client poll-retry <poll-retry>`

**Mode** Global Config

##### 4.7.6.1 no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

**Format** `no sntp unicast client poll-retry`

**Mode** Global Config



### 4.7.7 sntp 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

#### 4.7.7.1 no sntp server

This command deletes an server from the configured SNTP servers.

**Format** `no sntp server remove <ipaddress|hostname>`  
**Mode** Global Config

### 4.7.8 show sntp

This command is used to display SNTP settings and status.

**Format** `show sntp`  
**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Last Update Time</b>	Time of last clock update.
<b>Last Attempt Time</b>	Time of last transmit query (in unicast mode).
<b>Last Attempt Status</b>	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
<b>Broadcast Count</b>	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
<b>Multicast Count</b>	Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot.

### 4.7.9 show sntp client

This command is used to display SNTP client settings.

**Format** `show sntp client`  
**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Client Supported Modes</b>	Supported SNTP Modes (Broadcast, Unicast, or Multicast).
<b>SNTP Version</b>	The highest SNTP version the client supports.
<b>Port</b>	SNTP Client Port.
<b>Client Mode</b>	Configured SNTP Client Mode.





### 4.7.10 show sntp server

This command is used to display SNTP server settings and configured servers.

**Format**            `show sntp server`  
**Mode**              Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Server IP Address / Hostname</b>	IP address or hostname of configured SNTP Server.
<b>Server Type</b>	Address Type of Server.
<b>Server Stratum</b>	Claimed stratum of the server for the last received valid packet.
<b>Server Reference ID</b>	Reference clock identifier of the server for the last received valid packet.
<b>Server Mode</b>	SNTP Server mode.
<b>Server Maximum Entries</b>	Total number of SNTP Servers allowed.
<b>Server Current Entries</b>	Total number of SNTP configured.

For each configured server:

<i>Term</i>	<i>Definition</i>
<b>IP Address / Hostname</b>	IP address or hostname of configured SNTP Server.
<b>Address Type</b>	Address Type of configured SNTP server.
<b>Priority</b>	IP priority type of the configured server.
<b>Version</b>	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
<b>Port</b>	Server Port Number.
<b>Last Attempt Time</b>	Last server attempt time for the specified server.
<b>Last Update Status</b>	Last server attempt status for the server.
<b>Total Unicast Requests</b>	Number of requests to the server.
<b>Failed Unicast Requests</b>	Number of failed requests from server.

## 4.8 DHCP Server Commands

This section describes the commands you to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

### 4.8.1 ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode.

**Default**            none  
**Format**            `ip dhcp pool <name>`  
**Mode**              Global Config



#### 4.8.1.1 no ip dhcp pool

This command removes the DHCP address pool. The name should be previously configured pool name.

**Format** no ip dhcp pool *<name>*

**Mode** Global Config

#### 4.8.2 client-identifier

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique-identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, Assigned Numbers for a list of media type codes.

**Default** none

**Format** client-identifier *<uniqueidentifier>*

**Mode** DHCP Pool Config

#### 4.8.2.1 no client-identifier

This command deletes the client identifier.

**Format** no client-identifier

**Mode** DHCP Pool Config

#### 4.8.3 client-name

This command specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

**Default** none

**Format** client-name *<name>*

**Mode** DHCP Pool Config

#### 4.8.3.1 no client-name

This command removes the client name.

**Format** no client-name

**Mode** DHCP Pool Config

#### 4.8.4 default-router

This command specifies the default router list for a DHCP client. *{address1, address2... address8}* are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

**Default** none

**Format** default-router *<address1> [<address2>...<address8>]*

**Mode** DHCP Pool Config



#### 4.8.4.1 no default-router

This command removes the default router list.

**Format** no default-router

**Mode** DHCP Pool Config

#### 4.8.5 dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

**Default** none

**Format** dns-server <address1> [<address2>...<address8>]

**Mode** DHCP Pool Config

#### 4.8.5.1 no dns-server

This command removes the DNS Server list.

**Format** no dns-server

**Mode** DHCP Pool Config

#### 4.8.6 hardware-address

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

**Default** ethernet

**Format** hardware-address <hardwareaddress> <type>

**Mode** DHCP Pool Config

#### 4.8.6.1 no hardware-address

This command removes the hardware address of the DHCP client.

**Format** no hardware-address

**Mode** DHCP Pool Config

#### 4.8.7 host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32.

**Default** none

**Format** host <address> [{<mask> | <prefix-length>}]

**Mode** DHCP Pool Config



#### 4.8.7.1 no host

This command removes the IP address of the DHCP client.

**Format** no host  
**Mode** DHCP Pool Config

#### 4.8.8 lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If you specify *infinite*, the lease is set for 60 days. You can also specify a lease duration. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 23. *Minutes* is an integer from 0 to 59.

**Default** 1 (day)  
**Format** lease [*<days>* [*<hours>*] [*<minutes>*] | *infinite*]  
**Mode** DHCP Pool Config

#### 4.8.8.1 no lease

This command restores the default value of the lease time for DHCP Server.

**Format** no lease  
**Mode** DHCP Pool Config

#### 4.8.9 network (DHCP Pool Config)

Use this command to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

**Default** none  
**Format** network *<networknumber>* [*<mask>* | *<prefixlength>*]  
**Mode** DHCP Pool Config

#### 4.8.9.1 no network

This command removes the subnet number and mask.

**Format** no network  
**Mode** DHCP Pool Config

#### 4.8.10 bootfile

The command specifies the name of the default boot image for a DHCP client. The *<filename>* specifies the boot image file.

**Format** bootfile *<filename>*  
**Mode** DHCP Pool Config



#### 4.8.10.1 no bootfile

This command deletes the boot image name.

**Format** no bootfile  
**Mode** DHCP Pool Config

#### 4.8.11 domain-name

This command specifies the domain name for a DHCP client. The *<domain>* specifies the domain name string of the client.

**Default** none  
**Format** domain-name *<domain>*  
**Mode** DHCP Pool Config

#### 4.8.11.1 no domain-name

This command removes the domain name.

**Format** no domain-name  
**Mode** DHCP Pool Config

#### 4.8.12 netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

**Default** none  
**Format** netbios-name-server *<address>* [*<address2>*...*<address8>*]  
**Mode** DHCP Pool Config

#### 4.8.12.1 no netbios-name-server

This command removes the NetBIOS name server list.

**Format** no netbios-name-server  
**Mode** DHCP Pool Config

#### 4.8.13 netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients.type Specifies the NetBIOS node type. Valid types are:

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed



- h-node—Hybrid (recommended)

**Default** none  
**Format** `netbios-node-type <type>`  
**Mode** DHCP Pool Config

#### 4.8.13.1 no netbios-node-type

This command removes the NetBIOS node Type.

**Format** `no netbios-node-type`  
**Mode** DHCP Pool Config

### 4.8.14 next-server

This command configures the next server in the boot process of a DHCP client. The `<address>` parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

**Default** inbound interface helper addresses  
**Format** `next-server <address>`  
**Mode** DHCP Pool Config

#### 4.8.14.1 no next-server

This command removes the boot server list.

**Format** `no next-server`  
**Mode** DHCP Pool Config

### 4.8.15 option

The `option` command configures DHCP Server options. The `<code>` parameter specifies the DHCP option code and ranges from 1-254. The `<ascii string>` parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The `hex <string>` parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, `a3.4f.22.0c`), colon (for example, `a3:4f:22:0c`), or white space (for example, `a3 4f 22 0c`).

**Default** none  
**Format** `option <code> {ascii string | hex <string1> [<string2>...<string8>] | ip <address1> [<address2>...<address8>]}`  
**Mode** DHCP Pool Config

#### 4.8.15.1 no option

This command removes the DHCP Server options. The `<code>` parameter specifies the DHCP option code.

**Format** `no option <code>`  
**Mode** DHCP Pool Config



#### 4.8.16 ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

**Default** none  
**Format** `ip dhcp excluded-address <lowaddress> [highaddress]`  
**Mode** Global Config

##### 4.8.16.1 no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

**Format** `no ip dhcp excluded-address <lowaddress> [highaddress]`  
**Mode** Global Config

#### 4.8.17 ip dhcp ping packets

Use this command to specify the number, in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

**Default** 2  
**Format** `ip dhcp ping packets <0,2-10>`  
**Mode** Global Config

##### 4.8.17.1 no ip dhcp ping packets

This command prevents the server from pinging pool addresses and sets the number of packets to 0.

**Default** 0  
**Format** `no ip dhcp ping packets`  
**Mode** Global Config

#### 4.8.18 service dhcp

This command enables the DHCP server.

**Default** disabled  
**Format** `service dhcp`  
**Mode** Global Config

##### 4.8.18.1 no service dhcp

This command disables the DHCP server.

**Format** `no service dhcp`  
**Mode** Global Config



### 4.8.19 ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

**Default** disabled  
**Format** ip dhcp bootp automatic  
**Mode** Global Config

#### 4.8.19.1 no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

**Format** no ip dhcp bootp automatic  
**Mode** Global Config

### 4.8.20 ip dhcp conflict logging

This command enables conflict logging on DHCP server.

**Default** enabled  
**Format** ip dhcp conflict logging  
**Mode** Global Config

#### 4.8.20.1 no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

**Format** no ip dhcp conflict logging  
**Mode** Global Config

### 4.8.21 clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If "\*" is specified, the bindings corresponding to all the addresses are deleted. *<address>* is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

**Format** clear ip dhcp binding {*<address>* | \*}  
**Mode** Privileged EXEC

### 4.8.22 clear ip dhcp server statistics

This command clears DHCP server statistics counters.

**Format** clear ip dhcp server statistics  
**Mode** Privileged EXEC





### 4.8.23 clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If the asterisk (\*) character is used as the address parameter.

**Default** none  
**Format** `clear ip dhcp conflict {<address> | *}`  
**Mode** Privileged EXEC

### 4.8.24 show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

**Format** `show ip dhcp binding [<address>]`  
**Modes**

- Privileged EXEC
- User EXEC

<i>Term</i>	<i>Definition</i>
<b>IP address</b>	The IP address of the client.
<b>Hardware Address</b>	The MAC Address or the client identifier.
<b>Lease expiration</b>	The lease expiration time of the IP address assigned to the client.
<b>Type</b>	The manner in which IP address was assigned to the client.

### 4.8.25 show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

**Format** `show ip dhcp global configuration`  
**Modes**

- Privileged EXEC
- User EXEC

<i>Term</i>	<i>Definition</i>
<b>Service DHCP</b>	The field to display the status of dhcp protocol.
<b>Number of Ping Packets</b>	The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.
<b>Conflict Logging</b>	Shows whether conflict logging is enabled or disabled.
<b>BootP Automatic</b>	Shows whether BootP for dynamic pools is enabled or disabled.

### 4.8.26 show ip dhcp pool configuration

This command displays pool configuration. If `all` is specified, configuration for all the pools is displayed.

**Format** `show ip dhcp pool configuration {<name> | all}`  
**Modes**

- Privileged EXEC
- User EXEC



<i>Field</i>	<i>Definition</i>
<b>Pool Name</b>	The name of the configured pool.
<b>Pool Type</b>	The pool type.
<b>Lease Time</b>	The lease expiration time of the IP address assigned to the client.
<b>DNS Servers</b>	The list of DNS servers available to the DHCP client .
<b>Default Routers</b>	The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

<i>Field</i>	<i>Definition</i>
<b>Network</b>	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

<i>Field</i>	<i>Definition</i>
<b>Client Name</b>	The name of a DHCP client.
<b>Client Identifier</b>	The unique identifier of a DHCP client.
<b>Hardware Address</b>	The hardware address of a DHCP client.
<b>Hardware Address Type</b>	The protocol of the hardware platform.
<b>Host</b>	The IP address and the mask for a manual binding to a DHCP client.

#### 4.8.27 show ip dhcp server statistics

This command displays DHCP server statistics.

<b>Format</b>	<code>show ip dhcp server statistics</code>
<b>Modes</b>	<ul style="list-style-type: none"> <li>• Privileged EXEC</li> <li>• User EXEC</li> </ul>

<i>Field</i>	<i>Definition</i>
<b>Automatic Bindings</b>	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
<b>Expired Bindings</b>	The number of expired leases.
<b>Malformed Bindings</b>	The number of truncated or corrupted messages that were received by the DHCP server.

Message Received:

<i>Message</i>	<i>Definition</i>
<b>DHCP DISCOVER</b>	The number of DHCPDISCOVER messages the server has received.
<b>DHCP REQUEST</b>	The number of DHCPREQUEST messages the server has received.
<b>DHCP DECLINE</b>	The number of DHCPDECLINE messages the server has received.
<b>DHCP RELEASE</b>	The number of DHCPRELEASE messages the server has received.
<b>DHCP INFORM</b>	The number of DHCPINFORM messages the server has received.



Message Sent:

<b>Message</b>	<b>Definition</b>
<b>DHCP OFFER</b>	The number of DHCP OFFER messages the server sent.
<b>DHCP ACK</b>	The number of DHCP ACK messages the server sent.
<b>DHCP NACK</b>	The number of DHCP NACK messages the server sent.

#### 4.8.28 show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

**Format** `show ip dhcp conflict [<ip-address>]`

**Modes**

- Privileged EXEC
- User EXEC

<b>Term</b>	<b>Definition</b>
<b>IP address</b>	The IP address of the host as recorded on the DHCP server.
<b>Detection Method</b>	The manner in which the IP address of the hosts were found on the DHCP Server.
<b>Detection time</b>	The time when the conflict was found.

## 4.9 DHCP Filtering

You can configure the DHCP Filtering feature as a security measure against unauthorized DHCP servers. DHCP filtering works by allowing you to configure each port as either a trusted port or an untrusted port. To optimize the DHCP filtering feature, configure the port that is connected to an authorized DHCP server on your network as a trusted port. Any DHCP responses received on a trusted port are forwarded. Make sure that all other ports are untrusted so that any DHCP (or BootP) responses received are discarded.

You can configure DHCP filtering on physical ports and LAGs. DHCP filtering is not operable on VLAN interfaces.

### 4.9.1 ip dhcp filtering

This command enables DHCP filtering globally.

**Default** disabled

**Format** `ip dhcp filtering`

**Mode** Global Config

#### 4.9.1.1 no ip dhcp filtering

This command disables DHCP filtering.

**Format** `no ip dhcp filtering`

**Mode** Global Config



## 4.9.2 ip dhcp filtering trust

This command configures an interface as trusted.

**Default** untrusted  
**Format** ip dhcp filtering trust  
**Mode** Interface Config

### 4.9.2.1 no ip dhcp filtering trust

This command returns an interface to the default value for DHCP filtering.

**Format** no ip dhcp filtering trust  
**Mode** Interface Config

## 4.9.3 show ip dhcp filtering

This command displays the DHCP filtering configuration.

**Format** show ip dhcp filtering  
**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Interface</b>	The interface by slot/port.
<b>Trusted</b>	Indicates whether the interface is trusted or untrusted.

## 4.10 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.

### 4.10.1 ip domain lookup

Use this command to enable the DNS client.

**Default** enabled  
**Format** ip domain lookup  
**Mode** Global Config

#### 4.10.1.1 no ip domain lookup

Use this command to disable the DNS client.

**Format** no ip domain lookup  
**Mode** Global Config



### 4.10.2 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.

#### 4.10.2.1 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

### 4.10.3 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

#### 4.10.3.1 no ip domain list

Use this command to delete a name from a list.

**Format** `no ip domain list <name>`  
**Mode** Global Config

### 4.10.4 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



#### 4.10.4.1 no ip name server

Use this command to remove a name server.

**Format** no ip name-server [*server-address1...server-address8*]

**Mode** Global Config

#### 4.10.5 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

#### 4.10.5.1 no ip host

Use this command to remove the name-to-address mapping.

**Format** no ip host *<name>*

**Mode** Global Config

#### 4.10.6 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

#### 4.10.6.1 no ip domain retry

Use this command to return to the default.

**Format** no ip domain retry *<number>*

**Mode** Global Config

#### 4.10.7 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



#### 4.10.7.1 no ip domain timeout

Use this command to return to the default setting.

**Format**            `no ip domain timeout <seconds>`

**Mode**             Global Config

#### 4.10.8 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.

**Format**            `clear host {<name> | all}`

**Mode**             Privileged EXEC

<i>Field</i>	<i>Description</i>
<b>name</b>	A particular host entry to remove. <name> ranges from 1-255 characters.
<b>all</b>	Removes all entries.

#### 4.10.9 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

<i>Field</i>	<i>Description</i>
<b>Host Name</b>	Domain host name.
<b>Default Domain</b>	Default domain name.
<b>Default Domain List</b>	Default domain list.
<b>Domain Name Lookup</b>	DNS client enabled/disabled.
<b>Number of Retries</b>	Number of time to retry sending Domain Name System (DNS) queries.
<b>Retry Timeout Period</b>	Amount of time to wait for a response to a DNS query.
<b>Name Servers</b>	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

## 4.11 Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their FASTPATH product.



**Caution!** The output of “debug” commands can be long and may adversely affect system performance.

### 4.11.1 debug arp

Use this command to enable ARP debug protocol messages.

**Default** disabled  
**Format** `debug arp`  
**Mode** Privileged EXEC

#### 4.11.1.1 no debug arp

Use this command to disable ARP debug protocol messages.

**Format** `no debug arp`  
**Mode** Privileged EXEC

### 4.11.2 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

#### 4.11.2.1 no debug auto-voip

Use this command to disable Auto VOIP debug messages.

**Format** `no debug auto-voip`  
**Mode** Privileged EXEC





### 4.11.3 debug clear

This command disables all previously enabled “debug” traces.

<b>Default</b>	disabled
<b>Format</b>	<code>debug clear</code>
<b>Mode</b>	Privileged EXEC

### 4.11.4 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.

<b>Default</b>	disabled
<b>Format</b>	<code>debug console</code>
<b>Mode</b>	Privileged EXEC

#### 4.11.4.1 no debug console

This command disables the display of “debug” trace output on the login session in which it is executed.

<b>Format</b>	<code>no debug console</code>
<b>Mode</b>	Privileged EXEC

### 4.11.5 debug dot1x packet

Use this command to enable dot1x packet debug trace.

<b>Default</b>	disabled
<b>Format</b>	<code>debug dot1x</code>
<b>Mode</b>	Privileged EXEC

#### 4.11.5.1 no debug dot1x packet

Use this command to disable dot1x packet debug trace.

<b>Format</b>	<code>no debug dot1x</code>
<b>Mode</b>	Privileged EXEC

### 4.11.6 debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

<b>Default</b>	disabled
<b>Format</b>	<code>debug igmpsnooping packet</code>
<b>Mode</b>	Privileged EXEC



#### 4.11.6.1 no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

**Format**            `no debug igmpsnooping packet`  
**Mode**             Privileged EXEC

#### 4.11.7 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 IGMP Snooping [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:

<b>Parameter</b>	<b>Definition</b>
<b>TX</b>	A packet transmitted by the device.
<b>Intf</b>	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.
<b>Src_Mac</b>	Source MAC address of the packet.
<b>Dest_Mac</b>	Destination multicast MAC address of the packet.
<b>Src_IP</b>	The source IP address in the IP header in the packet.
<b>Dest_IP</b>	The destination multicast IP address in the packet.
<b>Type</b>	The type of IGMP packet. Type can be one of the following: <ul style="list-style-type: none"> <li>• <code>Membership_Query</code> – IGMP Membership Query</li> <li>• <code>V1_Membership_Report</code> – IGMP Version 1 Membership Report</li> <li>• <code>V2_Membership_Report</code> – IGMP Version 2 Membership Report</li> <li>• <code>V3_Membership_Report</code> – IGMP Version 3 Membership Report</li> <li>• <code>V2_Leave_Group</code> – IGMP Version 2 Leave Group</li> </ul>
<b>Group</b>	Multicast group address in the IGMP header.

#### 4.11.7.1 no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

**Format**            `no debug igmpsnooping transmit`  
**Mode**             Privileged EXEC



#### 4.11.8 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.

<b>Default</b>	disabled
<b>Format</b>	<b>debug igmpsnooping packet receive</b>
<b>Mode</b>	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMP Snooping [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:

<b>Parameter</b>	<b>Definition</b>
<b>RX</b>	A packet received by the device.
<b>Intf</b>	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.
<b>Src_Mac</b>	Source MAC address of the packet.
<b>Dest_Mac</b>	Destination multicast MAC address of the packet.
<b>Src_IP</b>	The source IP address in the ip header in the packet.
<b>Dest_IP</b>	The destination multicast ip address in the packet.
<b>Type</b>	The type of IGMP packet. Type can be one of the following: <ul style="list-style-type: none"> <li>• Membership_Query – IGMP Membership Query</li> <li>• V1_Membership_Report – IGMP Version 1 Membership Report</li> <li>• V2_Membership_Report – IGMP Version 2 Membership Report</li> <li>• V3_Membership_Report – IGMP Version 3 Membership Report</li> <li>• V2_Leave_Group – IGMP Version 2 Leave Group</li> </ul>
<b>Group</b>	Multicast group address in the IGMP header.

##### 4.11.8.1 no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

<b>Format</b>	<b>no debug igmpsnooping receive</b>
<b>Mode</b>	Privileged EXEC

#### 4.11.9 debug ip acl

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

<b>Default</b>	disabled
<b>Format</b>	<b>debug ip acl &lt;acl Number&gt;</b>
<b>Mode</b>	Privileged EXEC



#### 4.11.9.1 no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

**Format** no debug ip acl <acl Number>

**Mode** Privileged EXEC

#### 4.11.10 debug ip igmp packet

Use this command to trace IGMP packet reception and transmission. **receive** traces only received IGMP packets and **transmit** traces only transmitted IGMP packets. When neither keyword is used in the command, then all IGMP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

**Default** disabled

**Format** debug ip igmp packet [*receive|transmit*]

**Mode** Privileged EXEC

#### 4.11.10.1 no debug ip igmp packet

Use this command to disable debug tracing of IGMP packet reception and transmission.

**Format** no debug ip igmp packet [*receive|transmit*]

**Mode** Privileged EXEC

#### 4.11.11 debug ip mcache packet

Use this command for tracing MDATA packet reception and transmission. **receive** traces only received data packets and **transmit** traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

**Default** disabled

**Format** debug ip mcache packet [*receive|transmit*]

**Mode** Privileged EXEC

#### 4.11.11.1 no debug ip mcache packet

Use this command to disable debug tracing of MDATA packet reception and transmission.

**Format** no debug ip mcache packet [*receive|transmit*]

**Mode** Privileged EXEC

#### 4.11.12 debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

**Default** disabled



**Format**        `debug lacp packet`  
**Mode**            Privileged 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
```

#### 4.11.12.1      no debug lacp packet

This command disables tracing of LACP packets.

**Format**        `no debug lacp packet`  
**Mode**            Privileged EXEC

#### 4.11.13        debug mldsnopping packet

Use this command to trace MLD snooping packet reception and transmission. **receive** traces only received MLD snooping packets and **transmit** traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

**Default**        disabled  
**Format**        `debug mldsnopping packet [receive|transmit]`  
**Mode**            Privileged EXEC

#### 4.11.13.1      no debug mldsnopping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

#### 4.11.14        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:

<b>Parameter</b>	<b>Definition</b>
<b>TX/RX</b>	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
<b>Intf</b>	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.
<b>SRC_IP</b>	The source IP address in the IP header in the packet.
<b>DEST_IP</b>	The destination IP address in the IP header in the packet.
<b>Type</b>	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

#### 4.11.14.1 no debug ping packet

This command disables tracing of ICMP echo requests and responses.

**Format** no debug ping packet

**Mode** Privileged EXEC

#### 4.11.15 debug sflow packet

Use this command to enable sFlow debug packet trace.

**Default** disabled

**Format** debug sflow packet

**Mode** Privileged EXEC

#### 4.11.15.1 no debug sflow packet

Use this command to disable sFlow debug packet trace.

**Format** no debug sflow packet

**Mode** Privileged EXEC

#### 4.11.16 debug spanning-tree bpdu

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

**Default** disabled

**Format** debug spanning-tree bpdu

**Mode** Privileged EXEC

#### 4.11.16.1 no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

**Format** no debug spanning-tree bpdu

**Mode** Privileged EXEC



#### 4.11.17 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.

<b>Default</b>	disabled
<b>Format</b>	<code>debug spanning-tree bpdu receive</code>
<b>Mode</b>	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:

<b>Parameter</b>	<b>Definition</b>
<b>RX</b>	A packet received by the device.
<b>Intf</b>	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.
<b>Source_Mac</b>	Source MAC address of the packet.
<b>Version</b>	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
<b>Root_Mac</b>	MAC address of the CIST root bridge.
<b>Root_Priority</b>	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
<b>Path_Cost</b>	External root path cost component of the BPDU.

#### 4.11.17.1 no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

<b>Format</b>	<code>no debug spanning-tree bpdu receive</code>
<b>Mode</b>	Privileged EXEC

#### 4.11.18 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.

<b>Default</b>	disabled
<b>Format</b>	<code>debug spanning-tree bpdu transmit</code>
<b>Mode</b>	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:

<b>Parameter</b>	<b>Definition</b>
<b>TX</b>	A packet transmitted by the device.
<b>Intf</b>	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.
<b>Source_Mac</b>	Source MAC address of the packet.
<b>Version</b>	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
<b>Root_Mac</b>	MAC address of the CIST root bridge.
<b>Root_Priority</b>	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
<b>Path_Cost</b>	External root path cost component of the BPDU.

#### 4.11.18.1 no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

**Format** no debug spanning-tree bpdu transmit  
**Mode** Privileged EXEC

#### 4.11.19 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

#### 4.11.19.1 no logging persistent

Use this command to disable the persistent logging in the switch.

**Format** no logging persistent  
**Mode** Global Config

### 4.12 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.

#### 4.12.1 cablestatus

This command returns the status of the specified port.





**Format** `cablestatus <slot/port>`  
**Mode** Privileged EXEC

<i>Field</i>	<i>Description</i>
<b>Cable Status</b>	One of the following statuses is returned: <ul style="list-style-type: none"> <li>• <b>Normal:</b> The cable is working correctly.</li> <li>• <b>Open:</b> The cable is disconnected or there is a faulty connector.</li> <li>• <b>Short:</b> There is an electrical short in the cable.</li> <li>• <b>Cable Test Failed:</b> The cable status could not be determined. The cable may in fact be working.</li> </ul>
<b>Cable Length</b>	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.

## 4.13 sFlow Commands

sFlow<sup>®</sup> 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.

### 4.13.1 sflow receiver

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

**Format** `sflow receiver <rcvr_idx> owner <owner-string> timeout <rcvr_timeout>`  
`max datagram <size> ip/ipv6 <ip> port <port>`  
**Mode** Global Config

<i>Field</i>	<i>Description</i>
<b>Receiver Owner</b>	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.
<b>Receiver Timeout</b>	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0-4294967295 seconds. The default is zero (0).
<b>Receiver Max Datagram Size</b>	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 9116). The default is 1400.
<b>Receiver IP</b>	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. The default is 0.0.0.0.
<b>Receiver Port</b>	The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.



#### 4.13.1.1 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

#### 4.13.2 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.

**Format** `sflow sampler {<rcvr-idx> | rate <sampling-rate> | maxheadersize <size>}`

**Mode** Interface Config

Field	Description
Receiver Index	The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. A value of zero (0) means that no receiver is configured, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. Possible values are 1-8. The default is 0.
Maxheadersize	The maximum number of bytes that should be copied from the sampler packet. The range is 20-256. The default is 128. When set to zero (0), all the sampler parameters are set to their corresponding default value.
Sampling Rate	The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A value of zero (0) disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. The range is 1024-65536 and 0. The default is 0.

#### 4.13.2.1 no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

**Format** `no sflow sampler {<rcvr-idx> | rate <sampling-rate> | maxheadersize <size>}`

**Mode** Interface Config

#### 4.13.3 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.

**Format** `sflow poller {<rcvr-idx> | interval <poll-interval>}`

**Mode** Interface Config

Field	Description
Receiver Index	Enter the sFlow Receiver associated with the sampler/poller. A value of zero (0) means that no receiver is configured. The range is 1-8. The default is 0.



<i>Field</i>	<i>Description</i>
<b>Poll Interval</b>	Enter the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. When set to zero (0), all the poller parameters are set to their corresponding default value. The range is 0-86400. The default is 0. A value of N means once in N seconds a counter sample is generated.

#### 4.13.3.1 no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

**Format**            `no sflow poller {<rcvr-indx> | interval <poll-interval>}`  
**Mode**             Interface Config

#### 4.13.4 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.

**Format**            `show sflow agent`  
**Mode**             Privileged EXEC

<i>Field</i>	<i>Description</i>
<b>sFlow Version</b>	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: <ul style="list-style-type: none"> <li>• MIB Version: '1.3', the version of this MIB.</li> <li>• Organization: Broadcom Corp.</li> <li>• Revision: 1.0</li> </ul>
<b>IP Address</b>	The IP address associated with this agent.

**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.

**Format**            `show sflow pollers`  
**Mode**             Privileged EXEC

<i>Field</i>	<i>Description</i>
<b>Poller Data Source</b>	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
<b>Receiver Index</b>	The sFlowReceiver associated with this sFlow counter poller.
<b>Poller Interval</b>	The number of seconds between successive samples of the counters associated with this data source.



### 4.13.5 show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

**Format**            `show sflow receivers` [<index>]

**Mode**             Privileged EXEC

<i>Field</i>	<i>Description</i>
<b>Receiver Index</b>	The sFlow Receiver associated with the sampler/poller.
<b>Owner String</b>	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.
<b>Time Out</b>	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver.
<b>Max Datagram Size</b>	The maximum number of bytes that can be sent in a single sFlow datagram.
<b>Port</b>	The destination Layer4 UDP port for sFlow datagrams.
<b>IP Address</b>	The sFlow receiver IP address.
<b>Address Type</b>	The sFlow receiver IP address type. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.
<b>Datagram Version</b>	The sFlow protocol version to be used while sending samples to sFlow receiver.

**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
```

### 4.13.6 show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

**Format**            `show sflow samplers`

**Mode**             Privileged EXEC

<i>Field</i>	<i>Description</i>
<b>Sampler Data Source</b>	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
<b>Receiver Index</b>	The sFlowReceiver configured for this sFlow sampler.
<b>Packet Sampling Rate</b>	The statistical sampling rate for packet sampling from this source.
<b>Max Header Size</b>	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.



---

*Chapter*

---

**5**

---

# Management Commands

---



## 5. Management Commands

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

The Management Commands chapter contains the following sections:

- 5.1 “Network Interface Commands” on page 5 - 2.
- 5.2 “Console Port Access Commands” on page 5 - 5.
- 5.3 “Telnet Commands” on page 5 - 7.
- 5.4 “Secure Shell (SSH) Commands” on page 5 - 11.
- 5.5 “Management Security Commands” on page 5 - 13.
- 5.6 “Access Commands” on page 5 - 14.
- 5.7 “User Account Commands” on page 5 - 15.
- 5.8 “SNMP Commands” on page 5 - 20.
- 5.9 “RADIUS Commands” on page 5 - 32.
- 5.10 “TACACS+ Commands” on page 5 - 42.
- 5.11 “Configuration Scripting Commands” on page 5 - 45.
- 5.12 “Pre-login Banner and System Prompt Commands” on page 5 - 47.
- 5.13 “Diagnostics Commands” on page 5 - 47
- 5.14 “PCI express Commands” on page 5 - 47
- 5.15 “Storage Commands” on page 5 - 48
- 5.16 “Clock support commands” on page 5 - 48



**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.

### 5.1 Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see 2.3.2 “network mgmt\_vlan” on page 2 - 21

#### 5.1.1 enable (Privileged EXEC access)

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

**Format**            `enable`  
**Mode**             User EXEC

#### 5.1.2 serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port.

**Format**            `serviceport ip <ipaddr> <netmask> [gateway]`



**Mode** Privileged EXEC

### 5.1.3 serviceport protocol

This command specifies the network management port configuration protocol. If you modify this value, the change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

**Format** `serviceport protocol {none | bootp | dhcp}`

**Mode** Privileged EXEC

### 5.1.4 network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet.

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

**Mode** Privileged EXEC

### 5.1.5 network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

**Default** none

**Format** `network protocol {none | bootp | dhcp}`

**Mode** Privileged EXEC

### 5.1.6 network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

**Format** `network mac-address <macaddr>`

**Mode** Privileged EXEC



### 5.1.7 network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

**Default** burnedin  
**Format** network mac-type {local | burnedin}  
**Mode** Privileged EXEC

#### 5.1.7.1 no network mac-type

This command resets the value of MAC address to its default.

**Format** no network mac-type  
**Mode** Privileged EXEC

### 5.1.8 show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. 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
<b>IP Address</b>	The IP address of the interface. The factory default value is 0.0.0.0.
<b>Subnet Mask</b>	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
<b>Default Gateway</b>	The default gateway for this IP interface. The factory default value is 0.0.0.0.
<b>IPv6 Administrative Mode</b>	Whether enabled or disabled.
<b>IPv6 Address/Length</b>	The IPv6 address and length.
<b>IPv6 Default Router</b>	The IPv6 default router address.
<b>Burned In MAC Address</b>	The burned in MAC address used for in-band connectivity.
<b>Locally Administered MAC Address</b>	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 BridgIdentifier is formed which is used in the Spanning Tree Protocol.
<b>MAC Address Type</b>	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.





<b>Term</b>	<b>Definition</b>
<b>Network Configuration Protocol Current</b>	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
```

### 5.1.9 show serviceport

This command displays service port configuration information.

**Format**            `show serviceport`  
**Mode**              Privileged EXEC

<b>Term</b>	<b>Definition</b>
<b>IP Address</b>	The IP address of the interface. The factory default value is 0.0.0.0.
<b>Subnet Mask</b>	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
<b>Default Gateway</b>	The default gateway for this IP interface. The factory default value is 0.0.0.0.
<b>ServPort Configuration Protocol Current</b>	The network protocol used on the last, or current, power-up cycle, if any.
<b>Burned in MAC Address</b>	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
```

## 5.2 Console Port Access Commands

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.



### 5.2.1 configuration

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

**Format** configuration  
**Mode** Privileged EXEC

### 5.2.2 lineconfig

This command gives you access to the Line Config mode, which allows you to configure various Telnet settings and the console port.

**Format** lineconfig  
**Mode** Global Config

### 5.2.3 serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

**Default** 9600  
**Format** serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}  
**Mode** Line Config

#### 5.2.3.1 no serial baudrate

This command sets the communication rate of the terminal interface.

**Format** no serial baudrate  
**Mode** Line Config

### 5.2.4 serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

**Default** 5  
**Format** serial timeout <0-160>  
**Mode** Line Config

#### 5.2.4.1 no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

**Format** no serial timeout  
**Mode** Line Config



### 5.2.5 show serial

This command displays serial communication settings for the switch.

**Format**            `show serial`  
**Modes**            • Privileged EXEC  
                       • User EXEC

<i>Term</i>	<i>Definition</i>
<b>Serial Port Login Timeout (minutes)</b>	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.
<b>Baud Rate (bps)</b>	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.
<b>Character Size (bits)</b>	The number of bits in a character. The number of bits is always 8.
<b>Flow Control</b>	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
<b>Stop Bits</b>	The number of Stop bits per character. The number of Stop bits is always 1.
<b>Parity Type</b>	The Parity Method used on the Serial Port. The Parity Method is always None.

## 5.3 Telnet Commands

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

### 5.3.1 ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

**Default**            enabled  
**Format**            `ip telnet server enable`  
**Mode**              Privileged EXEC

#### 5.3.1.1 no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

**Format**            `no ip telnet server enable`  
**Mode**              Privileged EXEC

### 5.3.2 telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address 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

### 5.3.3 transport input telnet

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.



**Note:** If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the `ip telnet server enable` command to enable Telnet Server Admin Mode.

**Default** enabled

**Format** `transport input telnet`

**Mode** Line Config

#### 5.3.3.1 no transport input telnet

Use this command to prevent new Telnet sessions from being established.

**Format** `no transport input telnet`

**Mode** Line Config

### 5.3.4 transport output telnet

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

**Default** enabled

**Format** `transport output telnet`

**Mode** Line Config

#### 5.3.4.1 no transport output telnet

Use this command to prevent new outbound Telnet connection from being established.

**Format** `no transport output telnet`

**Mode** Line Config



### 5.3.5 session-limit

This command specifies the maximum number of simultaneous outbound Telnet sessions. A value of 0 indicates that no outbound Telnet session can be established.

**Default** 5  
**Format** `session-limit <0-5>`  
**Mode** Line Config

#### 5.3.5.1 no session-limit

This command sets the maximum number of simultaneous outbound Telnet sessions to the default value.

**Format** `no session-limit`  
**Mode** Line Config

### 5.3.6 session-timeout

This command sets the Telnet session timeout value. The timeout value unit of time is minutes.

**Default** 5  
**Format** `session-timeout <1-160>`  
**Mode** Line Config

#### 5.3.6.1 no session-timeout

This command sets the Telnet session timeout value to the default. The timeout value unit of time is minutes.

**Format** `no session-timeout`  
**Mode** Line Config

### 5.3.7 telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

**Default** 5  
**Format** `telnetcon maxsessions <0-5>`  
**Mode** Privileged EXEC

#### 5.3.7.1 no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

**Format** `no telnetcon maxsessions`  
**Mode** Privileged EXEC



## 5.3.8 telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.



**Note:** When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

**Default** 5  
**Format** `telnetcon timeout <1-160>`  
**Mode** Privileged EXEC

### 5.3.8.1 no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.



**Note:** Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration.

**Format** `no telnetcon timeout`  
**Mode** Privileged EXEC

## 5.3.9 show telnet

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system.

**Format** `show telnet`  
**Modes**

- Privileged EXEC
- User EXEC

<i>Term</i>	<i>Definition</i>
<b>Outbound Telnet Login Timeout</b>	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
<b>Maximum Number of Outbound Telnet Sessions</b>	The number of simultaneous outbound Telnet connections allowed.
<b>Allow New Outbound Telnet Sessions</b>	Indicates whether outbound Telnet sessions will be allowed.

### 5.3.10 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

<i>Term</i>	<i>Definition</i>
<b>Remote Connection Login Timeout (minutes)</b>	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.
<b>Maximum Number of Remote Connection Sessions</b>	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
<b>Allow New Telnet Sessions</b>	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

## 5.4 Secure Shell (SSH) Commands

This section describes the commands you use to configure SSH access to the switch. Use SSH to access the switch from a remote management host.



**Note:** The system allows a maximum of 5 SSH sessions.

### 5.4.1 ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the `ip ssh server enable` command.)

<b>Default</b>	disabled
<b>Format</b>	<code>ip ssh</code>
<b>Mode</b>	Privileged EXEC

### 5.4.2 ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

<b>Default</b>	1 and 2
<b>Format</b>	<code>ip ssh protocol [1] [2]</code>
<b>Mode</b>	Privileged EXEC

### 5.4.3 ip ssh server enable

This command enables the IP secure shell server.

<b>Default</b>	disabled
<b>Format</b>	<code>ip ssh server enable</code>
<b>Mode</b>	Privileged EXEC

#### 5.4.3.1 no ip ssh server enable

This command disables the IP secure shell server.

<b>Format</b>	<code>no ip ssh server enable</code>
---------------	--------------------------------------



**Mode** Privileged EXEC

#### 5.4.4 sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

**Default** 5

**Format** `sshcon maxsessions <0-5>`

**Mode** Privileged EXEC

##### 5.4.4.1 no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

**Format** `no sshcon maxsessions`

**Mode** Privileged EXEC

#### 5.4.5 sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

**Default** 5

**Format** `sshcon timeout <1-160>`

**Mode** Privileged EXEC

##### 5.4.5.1 no sshcon timeout

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

**Format** `no sshcon timeout`

**Mode** Privileged EXEC

#### 5.4.6 show ip ssh

This command displays the ssh settings.

**Format** `show ip ssh`

**Mode** Privileged EXEC





<b>Term</b>	<b>Definition</b>
<b>Administrative Mode</b>	This field indicates whether the administrative mode of SSH is enabled or disabled.
<b>Protocol Level</b>	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
<b>SSH Sessions Currently Active</b>	The number of SSH sessions currently active.
<b>Max SSH Sessions Allowed</b>	The maximum number of SSH sessions allowed.
<b>SSH Timeout</b>	The SSH timeout value in minutes.
<b>Keys Present</b>	Indicates whether the SSH RSA and DSA key files are present on the device.
<b>Key Generation in Progress</b>	Indicates whether RSA or DSA key files generation is currently in progress.

## 5.5 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.

### 5.5.1 **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

#### 5.5.1.1 **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

### 5.5.2 **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

#### 5.5.2.1 **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



### 5.5.3 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

#### 5.5.3.1 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

## 5.6 Access Commands

Use the commands in this section to close remote connections or to view information about connections to the system.

### 5.6.1 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

### 5.6.2 show loginsession

This command displays current Telnet and serial port connections to the switch.

**Format**            `show loginsession`

**Mode**             Privileged EXEC

<b>Term</b>	<b>Definition</b>
<b>ID</b>	Login Session ID.
<b>User Name</b>	The name the user entered to log on to the system.
<b>Connection From</b>	IP address of the remote client machine or EIA-232 for the serial port connection.
<b>Idle Time</b>	Time this session has been idle.
<b>Session Time</b>	Total time this session has been connected.
<b>Session Type</b>	Shows the type of session, which can be telnet, serial, or SSH.



## 5.7 User Account Commands

This section describes the commands you use to add, manage, and delete system users. FASTPATH software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.



**Note:** You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

### 5.7.1 users name

This command adds a new user account, if space permits. The account `<username>` can be up to eight characters in length. You can use alphanumeric characters as well as the dash ('-') and underscore ('\_'). You can define up to six user names.



**Note:** The `<username>` is not case sensitive when you add and delete users, and when the user logs in. However, when you use the `<username>` to set the user password, authentication, or encryption, you must enter the `<username>` in the same case you used when you added the user. To see the case of the `<username>`, enter the `show users` command.

**Format**            `users name <username>`  
**Mode**             Global Config

#### 5.7.1.1 no users name

This command removes a user account.

**Format**            `no users name <username>`  
**Mode**             Global Config



**Note:** You cannot delete the "admin" user account.

### 5.7.2 users name <username> unlock

Use this command to unlock a locked user account. Only a user with read/write access can re-activate a locked user account.

**Format**            `users name <username> unlock`  
**Mode**             Global Config

### 5.7.3 users passwd

Use this command to change a password. Passwords are a maximum of 64 alphanumeric characters. If a user is authorized for authentication or encryption is enabled, the password length must be at least eight alphanumeric characters. The password is case sensitive. When you change a password, a prompt asks for the old password. If



there is no password, press enter. You must enter the `<username>` in the same case you used when you added the user. To see the case of the `<username>`, enter the `show users` command.



**Note:** To specify a blank password in the configuration script, you must specify it as a space within quotes, for example, " ". For more information about creating configuration scripts, see 5.11 "Configuration Scripting Commands" on page 5 - 45.

**Default** no password  
**Format** `users passwd <username>`  
**Mode** Global Config

### 5.7.3.1 no users passwd

This command sets the password of an existing user to blank. When you change a password, a prompt asks for the old password. If there is no password, press enter.

**Format** `no users passwd <username>`  
**Mode** Global Config

### 5.7.4 users passwd <username> encrypted <password>

This command allows the administrator to transfer local user passwords between devices without having to know the passwords. The `<password>` parameter must be exactly 128 hexadecimal characters. The user represented by the `<username>` parameter must be a pre-existing local user.

**Format** `users passwd <username> encrypted <password>`  
**Mode** Global Config

### 5.7.5 users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are `readonly` or `readwrite`. The `<username>` is the login user name for which the specified access mode applies. The default is `readwrite` for the "admin" user and `readonly` for all other users. You must enter the `<username>` in the same case you used when you added the user. To see the case of the `<username>`, enter the `show users` command.

**Defaults**

- admin - readwrite
- other - readonly

**Format** `users snmpv3 accessmode <username> {readonly | readwrite}`  
**Mode** Global Config

#### 5.7.5.1 no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified user as `readwrite` for the "admin" user and `readonly` for all other users. The `<username>` value is the user name for which the specified access mode will apply.

**Format** `no users snmpv3 accessmode <username>`  
**Mode** Global Config



### 5.7.6 users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are **none**, **md5** or **sha**. If you specify **md5** or **sha**, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The `<username>` is the user name associated with the authentication protocol. You must enter the `<username>` in the same case you used when you added the user. To see the case of the `<username>`, enter the **show users** command.

**Default** no authentication  
**Format** `users snmpv3 authentication <username> {none | md5 | sha}`  
**Mode** Global Config

#### 5.7.6.1 no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified user to **none**. The `<username>` is the user name for which the specified authentication protocol is used.

**Format** `no users snmpv3 authentication <username>`  
**Mode** Global Config

### 5.7.7 users snmpv3 encryption

This command specifies the encryption protocol used for the specified user. The valid encryption protocols are **des** or **none**.

If you select **des**, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the **des** protocol but do not provide a key, the user is prompted for the key. When you use the **des** protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select **none**, you do not need to provide a key.

The `<username>` value is the login user name associated with the specified encryption. You must enter the `<username>` in the same case you used when you added the user. To see the case of the `<username>`, enter the **show users** command.

**Default** no encryption  
**Format** `users snmpv3 encryption <username> {none | des[key]}`  
**Mode** Global Config

#### 5.7.7.1 no users snmpv3 encryption

This command sets the encryption protocol to **none**. The `<username>` is the login user name for which the specified encryption protocol will be used.

**Format** `no users snmpv3 encryption <username>`  
**Mode** Global Config



### 5.7.8 show users

This command displays the configured user names and their settings. This command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

**Format**            `show users`  
**Mode**             Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>User Name</b>	The name the user enters to login using the serial port, Telnet or Web.
<b>Access Mode</b>	Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the “admin” user has Read/Write access and the “guest” has Read Only access. There can only be one Read/Write user and up to five Read Only users.
<b>SNMPv3 Access Mode</b>	The SNMPv3 Access Mode. If the value is set to <code>ReadWrite</code> , the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to <code>ReadOnly</code> , the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.
<b>SNMPv3 Authentication</b>	The authentication protocol to be used for the specified login user.
<b>SNMPv3 Encryption</b>	The encryption protocol to be used for the specified login user.

### 5.7.9 show users accounts

This command displays the local user status with respect to user account lockout and password aging.

**Format**            `show users accounts`  
**Mode**             Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>User Name</b>	The local user account’s user name.
<b>Access Mode</b>	The user’s access level (read-only or read/write).
<b>Lockout Status</b>	Indicates whether the user account is locked out (true or false).
<b>Password Expiration Date</b>	The current password expiration date in date format.

### 5.7.10 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



### 5.7.11 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

#### 5.7.11.1 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

### 5.7.12 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

#### 5.7.12.1 no passwords history

Use this command to set the password history to the default value.

**Format** `no passwords history`  
**Mode** Global Config

### 5.7.13 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

#### 5.7.13.1 no passwords aging

Use this command to set the password aging to the default value.

**Format** `no passwords aging`  
**Mode** Global Config



### 5.7.14 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

#### 5.7.14.1 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

### 5.7.15 show passwords configuration

Use this command to display the configured password management settings.

**Format** `show passwords configuration`  
**Mode** Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Minimum Password Length</b>	Minimum number of characters required when changing passwords.
<b>Password History</b>	Number of passwords to store for reuse prevention.
<b>Password Aging</b>	Length in days that a password is valid.
<b>Lockout Attempts</b>	Number of failed password login attempts before lockout.

### 5.7.16 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

## 5.8 SNMP Commands

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.





### 5.8.1 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.

<b>Default</b>	none
<b>Format</b>	<b>snmp-server</b> {sysname <i>&lt;name&gt;</i>   location <i>&lt;loc&gt;</i>   contact <i>&lt;con&gt;</i> }
<b>Mode</b>	Global Config

### 5.8.2 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.

<b>Default</b>	<ul style="list-style-type: none"> <li>• Public and private, which you can rename.</li> <li>• Default values for the remaining four community names are blank.</li> </ul>
<b>Format</b>	<b>snmp-server community</b> <i>&lt;name&gt;</i>
<b>Mode</b>	Global Config

#### 5.8.2.1 no snmp-server community

This command removes this community name from the table. The *<name>* is the community name to be deleted.

<b>Format</b>	<b>no snmp-server community</b> <i>&lt;name&gt;</i>
<b>Mode</b>	Global Config

### 5.8.3 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.

<b>Default</b>	0.0.0.0
<b>Format</b>	<b>snmp-server community ipaddr</b> <i>&lt;ipaddr&gt;</i> <i>&lt;name&gt;</i>
<b>Mode</b>	Global Config

#### 5.8.3.1 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.

<b>Format</b>	<b>no snmp-server community ipaddr</b> <i>&lt;name&gt;</i>
<b>Mode</b>	Global Config



### 5.8.4 snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

**Default** 0.0.0.0  
**Format** `snmp-server community ipmask <ipmask> <name>`  
**Mode** Global Config

#### 5.8.4.1 no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

**Format** `no snmp-server community ipmask <name>`  
**Mode** Global Config

### 5.8.5 snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

**Default**

- private and public communities - enabled
- other four - disabled

**Format** `snmp-server community mode <name>`  
**Mode** Global Config

#### 5.8.5.1 no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

**Format** `no snmp-server community mode <name>`  
**Mode** Global Config

### 5.8.6 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

### 5.8.7 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 - 34.

**Default** disabled  
**Format** `snmp-server enable traps violation`  
**Mode** Interface Config

#### 5.8.7.1 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

### 5.8.8 snmp-server enable traps

This command enables the Authentication Flag.

**Default** enabled  
**Format** `snmp-server enable traps`  
**Mode** Global Config

#### 5.8.8.1 no snmp-server enable traps

This command disables the Authentication Flag.

**Format** `no snmp-server enable traps`  
**Mode** Global Config



### 5.8.9 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 5 - 26.

**Default**            enabled  
**Format**            `snmp-server enable traps linkmode`  
**Mode**              Global Config

#### 5.8.9.1 no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

**Format**            `no snmp-server enable traps linkmode`  
**Mode**              Global Config

### 5.8.10 snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

**Default**            enabled  
**Format**            `snmp-server enable traps multiusers`  
**Mode**              Global Config

#### 5.8.10.1 no snmp-server enable traps multiusers

This command disables Multiple User traps.

**Format**            `no snmp-server enable traps multiusers`  
**Mode**              Global Config

### 5.8.11 snmp-server enable traps pll

This command enables the generation of traps in case a PLL status change has occurred.

**Default**            enabled  
**Format**            `snmp-server enable traps pll`  
**Mode**              Global Config

#### 5.8.11.1 no snmp-server enable traps pll

This command disables the generation of traps in case a PLL status change has occurred.

**Format**            `no snmp-server enable traps pll`  
**Mode**              Global Config



### 5.8.12 snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

<b>Default</b>	enabled
<b>Format</b>	<code>snmp-server enable traps stpmode</code>
<b>Mode</b>	Global Config

#### 5.8.12.1 no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

<b>Format</b>	<code>no snmp-server enable traps stpmode</code>
<b>Mode</b>	Global Config

### 5.8.13 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.

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 implicitly set by specifying 'inform request'.

**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 page 5 - 21.

<b>Format</b>	<code>snmptrap &lt;name&gt; ipaddr &lt;ipaddr&gt;</code> <code>snmptrap &lt;name&gt; ipaddr &lt;ipaddr&gt; snmpversion {snmpv1   snmpv2}</code> <code>snmptrap &lt;name&gt; ipaddr &lt;ipaddr&gt; notification {trap   inform}</code>
<b>Mode</b>	Global Config

#### 5.8.13.1 no snmptrap

This command deletes trap receivers for a community.

<b>Format</b>	<code>no snmptrap &lt;name&gt; &lt;ipaddr&gt;</code>
<b>Mode</b>	Global Config



### 5.8.14 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

### 5.8.15 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

### 5.8.16 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

#### 5.8.16.1 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

### 5.8.17 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 5 - 24.

**Format** `snmp trap link-status`  
**Mode** Interface Config



### 5.8.17.1 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

### 5.8.18 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 5 - 24.

**Format**            `snmp trap link-status all`  
**Mode**                Global Config

### 5.8.18.1 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 5 - 24.

**Format**            `no snmp trap link-status all`  
**Mode**                Global Config

### 5.8.19 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

<i>Term</i>	<i>Definition</i>
<b>SNMP Community Name</b>	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.



<b>Term</b>	<b>Definition</b>
<b>Client IP Address</b>	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.
<b>Client IP Mask</b>	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.
<b>Access Mode</b>	The access level for this community string.
<b>Status</b>	The status of this community access entry.

### 5.8.20 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

<b>Term</b>	<b>Definition</b>
<b>SNMP Trap Name</b>	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.
<b>IP Address</b>	The IPv4 address to receive SNMP traps from this device.
<b>IPv6 Address</b>	The IPv6 address to receive SNMP traps from this device.
<b>SNMP Version</b>	SNMPv2
<b>Mode</b>	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
```

### 5.8.21 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

<b>Term</b>	<b>Definition</b>
<b>Authentication Flag</b>	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.





<b>Term</b>	<b>Definition</b>
<b>Link Up/Down Flag</b>	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
<b>Multiple Users Flag</b>	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).
<b>Spanning Tree Flag</b>	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
<b>ACL Traps</b>	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
<b>PLL clock trap</b>	Can be enabled or disabled. The factory default is disabled. Indicates a PLL state change.

### 5.8.22 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

### 5.8.23 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

### 5.8.24 show snmp-engine-id

This command displays the algorithm used to generate the Snmp-Engine-ID. It displays the configured and the currently active algorithm. A configured algorithm will become active after the next system reboot.

**Format** `show snmp-engine-id`  
**Mode** Privileged Exec

### 5.8.25 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')..

**Format** `set board snmp site {local | <ipmb-address>}`



**Mode** Privileged Exec

### 5.8.25.1 no set board snmp site

This command resets the sites used to monitor IPMI information via SNMP.

**Format** `no set board snmp site {local | <ipmb-address>}`

**Mode** Privileged Exec

### 5.8.26 show boardinfo snmp site

This command displays the sites used to monitor IPMI information via SNMP. The sites are indicated by 'local' for the local site and by the IPMB address for remote sites..

**Format** `show boardinfo snmp site`

**Mode** Privileged Exec

### 5.8.27 set board snmp ipmi-trap

This command enables/disables the generation of IPMI traps. If enabled, IPMI traps are sent if no filter (see below) exists or one filter rule fits..

**Format** `set board snmp ipmi-trap {enable | disable}`

**Mode** Privileged Exec

### 5.8.28 set board snmp ipmi-trap interval

This command specified the monitoring interval in seconds. The IPMI SEL is read and checked for generation of IPMI traps after each interval. The default is 30 seconds..

**Format** `set board snmp ipmi-trap interval <1..600>`

**Mode** Privileged Exec

### 5.8.29 set board snmp ipmi-trap filter

This command specified filter rules. It is checked for each SEL entry whether a specified rule fits. In this case a IPMI trap is sent. 20 rules can be specified..

**Format** `set board snmp ipmi-trap filter <1..20>`

**Mode** Privileged Exec

#### 5.8.29.1 no set board snmp ipmi-trap filter

This command resets filter rules.

**Format** `no set board snmp ipmi-trap filter <1..20>`

**Mode** Privileged Exec



### 5.8.30 enable (filter)

This command enables the filter rule..

**Format**            `enable`  
**Mode**              IPMI-filter Exec

### 5.8.31 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

### 5.8.32 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

### 5.8.33 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

### 5.8.34 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-recoverable}`  
**Mode**              IPMI-filter Exec

### 5.8.35 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



### 5.8.36 show boardinfo snmp ipmi-trap

This command displays the settings for generation of IPMI traps. It displays the general setting as well as all filter rules..

**Format** show boardinfo snmp ipmi-trap

**Mode** Privileged Exec

## 5.9 RADIUS Commands

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

### 5.9.1 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

#### 5.9.1.1 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

### 5.9.2 radius accounting mode

This command is used to enable the RADIUS accounting function.

**Default** disabled

**Format** radius accounting mode

**Mode** Global Config

#### 5.9.2.1 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

### 5.9.3 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.

### 5.9.3.1 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
```

### 5.9.4 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.

#### 5.9.4.1 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
```

#### 5.9.5 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

<i>Field</i>	<i>Description</i>
<b>ipaddr</b>	The IP address of the server.
<b>dnsname</b>	The DNS name of the server.
<b>password</b>	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>
```

## 5.9.6 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

<i>Field</i>	<i>Description</i>
<b>ip addr</b>	The IP address of the server.
<b>dnsname</b>	The DNS name of the server.

### 5.9.6.1 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

## 5.9.7 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

<i>Field</i>	<i>Description</i>
<b>ip addr</b>	The IP address of the RADIUS Authenticating server.
<b>dnsname</b>	The DNS name of the server.



### 5.9.8 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.

#### 5.9.8.1 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

### 5.9.9 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>.

#### 5.9.9.1 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

### 5.9.10 show radius

This command displays the values configured for the global parameters of the RADIUS client.

**Format** `show radius`





Mode Privileged EXEC

Term	Definition
<b>Number of Configured Authentication Servers</b>	The number of RADIUS Authentication servers that have been configured.
<b>Number of Configured Accounting Servers</b>	The number of RADIUS Accounting servers that have been configured.
<b>Number of Named Authentication Server Groups</b>	The number of configured named RADIUS server groups.
<b>Number of Named Accounting Server Groups</b>	The number of configured named RADIUS server groups.
<b>Number of Retransmits</b>	The configured value of the maximum number of times a request packet is retransmitted.
<b>Time Duration</b>	The configured timeout value, in seconds, for request re-transmissions.
<b>RADIUS Accounting Mode</b>	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
<b>RADIUS Attribute 4 Mode</b>	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
<b>RADIUS Attribute 4 Value</b>	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
```

### 5.9.11 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
<b>ipaddr</b>	The IP address of the authenticating server.
<b>dnsname</b>	The DNS name of the authenticating server.
<b>servername</b>	The alias name to identify the server.
<b>Current</b>	The '*' symbol preceding the server host address specifies that the server is currently active.
<b>Host Address</b>	The IP address of the host.



Field	Description
<b>Server Name</b>	The name of the authenticating server.
<b>Port</b>	The port used for communication with the authenticating server.
<b>Type</b>	Specifies whether this server is a primary or secondary type.
<b>Current Host Address</b>	The IP address of the currently active authenticating server.
<b>Secret Configured</b>	Yes or No Boolean value that indicates whether this server is configured with a secret.
<b>Number of Retransmits</b>	The configured value of the maximum number of times a request packet is retransmitted.
<b>Message Authenticator</b>	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
<b>Time Duration</b>	The configured timeout value, in seconds, for request retransmissions.
<b>RADIUS Accounting Mode</b>	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
<b>RADIUS Attribute 4 Mode</b>	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
<b>RADIUS Attribute 4 Value</b>	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
*	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
    
```

### 5.9.12 show radius accounting

This command displays a summary of configured RADIUS accounting servers.

**Format** `show radius accounting name [<servername>]`  
**Mode** Privileged EXEC

Field	Description
<b>servername</b>	An alias name to identify the server.
<b>RADIUS Accounting Mode</b>	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
<b>Host Address</b>	The IP address of the host.
<b>Server Name</b>	The name of the accounting server.
<b>Port</b>	The port used for communication with the accounting server.
<b>Secret Configured</b>	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
    
```



### 5.9.13 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

<i>Term</i>	<i>Definition</i>
<b>ipaddr</b>	The IP address of the server.
<b>dnsname</b>	The DNS name of the server.
<b>servername</b>	The alias name to identify the server.
<b>RADIUS Accounting Server Name</b>	The name of the accounting server.
<b>Server Host Address</b>	The IP address of the host.
<b>Round Trip Time</b>	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.
<b>Requests</b>	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
<b>Retransmission</b>	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
<b>Responses</b>	The number of RADIUS packets received on the accounting port from this server.
<b>Malformed Responses</b>	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.
<b>Bad Authenticators</b>	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
<b>Pending Requests</b>	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
<b>Timeouts</b>	The number of accounting timeouts to this server.
<b>Unknown Types</b>	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
<b>Packets Dropped</b>	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
```

### 5.9.14 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

<b>Term</b>	<b>Definition</b>
<b>ipaddr</b>	The IP address of the server.
<b>dnsname</b>	The DNS name of the server.
<b>servername</b>	The alias name to identify the server.
<b>RADIUS Server Name</b>	The name of the authenticating server.
<b>Server Host Address</b>	The IP address of the host.
<b>Access Requests</b>	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
<b>Access Retransmissions</b>	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
<b>Access Accepts</b>	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
<b>Access Rejects</b>	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
<b>Access Challenges</b>	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
<b>Malformed Access Responses</b>	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.
<b>Bad Authenticators</b>	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
<b>Pending Requests</b>	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
<b>Timeouts</b>	The number of authentication timeouts to this server.
<b>Unknown Types</b>	The number of packets of unknown type that were received from this server on the authentication port.



<i>Term</i>	<i>Definition</i>
<b>Packets Dropped</b>	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
```

## 5.10 TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

### 5.10.1 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

### 5.10.1.1 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

## 5.10.2 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

### 5.10.2.1 no tacacs-server key

Use the **no tacacs-server key** command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *<key-string>* parameter has a range of 0 - 128 characters. This key must match the key used on the TACACS+ daemon.

**Format** **no tacacs-server key** *<key-string>*

**Mode** Global Config

## 5.10.3 tacacs-server timeout

Use the **tacacs-server timeout** command to set the timeout value for communication with the TACACS+ servers. The *<timeout>* parameter has a range of 1-30 and is the timeout value in seconds.

**Default** 5

**Format** **tacacs-server timeout** *<timeout>*

**Mode** Global Config

### 5.10.3.1 no tacacs-server timeout

Use the **no tacacs-server timeout** command to restore the default timeout value for all TACACS servers.

**Format** **no tacacs-server timeout**

**Mode** Global Config



### 5.10.4 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

### 5.10.5 port

Use the **port** command in TACACS Configuration mode to specify a server port number. The server *<port-number>* range is 0 - 65535.

**Default**          49  
**Format**           **port** *<port-number>*  
**Mode**             TACACS Config

### 5.10.6 priority

Use the **priority** command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The *<priority>* parameter specifies the priority for servers. The highest priority is 0 (zero), and the range is 0 - 65535.

**Default**          0  
**Format**           **priority** *<priority>*  
**Mode**             TACACS Config

### 5.10.7 timeout

Use the **timeout** command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used. The *<timeout>* parameter has a range of 1-30 and is the timeout value in seconds.

**Format**           **timeout** *<timeout>*  
**Mode**             TACACS Config

### 5.10.8 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





<i>Term</i>	<i>Definition</i>
<b>IP address or Hostname</b>	The IP address or hostname of the configured TACACS+ server.
<b>Port</b>	The configured TACACS+ server port number.
<b>TimeOut</b>	The timeout in seconds for establishing a TCP connection.
<b>Priority</b>	The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.

## 5.11 Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the `show running-config` command (see 4.4.9 “show running-config” on page 4 - 15) to capture the running configuration into a script. Use the `copy` command (see 4.6.16 “copy” on page 4 - 29) to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- The file extension must be “.scr”.
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the “!” character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```



**Note:** To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user `jane` from a blank password to `hello`, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```



### 5.11.1 script apply

This command applies the commands in the script to the switch. The *<scriptname>* parameter is the name of the script to apply.

**Format**            `script apply <scriptname>`

**Mode**             Privileged EXEC

### 5.11.2 script delete

This command deletes a specified script where the *<scriptname>* parameter is the name of the script to delete. The *<all>* option deletes all the scripts present on the switch.

**Format**            `script delete {<scriptname> | all}`

**Mode**             Privileged EXEC

### 5.11.3 script list

This command lists all scripts present on the switch as well as the remaining available space.

**Format**            `script list`

**Mode**             Global Config

<i>Term</i>	<i>Definition</i>
<b>Configuration Script</b>	Name of the script.
<b>Size</b>	Privileged EXEC

### 5.11.4 script show

This command displays the contents of a script file, which is named *<scriptname>*.

**Format**            `script show <scriptname>`

**Mode**             Privileged EXEC

<i>Term</i>	<i>Definition</i>
<b>Output Format</b>	<code>line &lt;number&gt;: &lt;line contents&gt;</code>

### 5.11.5 script validate

This command validates a script file by parsing each line in the script file where *<scriptname>* is the name of the script to validate. The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

**Format**            `script validate <scriptname>`

**Mode**             Privileged EXEC



## 5.12 Pre-login Banner and System Prompt Commands

This section describes the commands you use to configure the pre-login banner and the system prompt. The pre-login banner is the text that displays before you login at the `user:` prompt.

### 5.12.1 copy (pre-login banner)

The `copy` command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using TFTP, Xmodem, Ymodem, or Zmodem.

**Default** none

**Format** `copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:clibanner`  
`copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>`

**Mode** Privileged EXEC

### 5.12.2 set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

**Format** `set prompt <prompt_string>`

**Mode** Privileged EXEC

## 5.13 Diagnostics Commands

### 5.13.1 diagnostics

This command will start diagnostics. If “interactive” is specified the switch will be restarted and the diagnostics loaded. The user gets a menu to select interactively a scenario. A serial console is needed. Otherwise, if a scenario is specified, this scenario is executed directly. You may start this scenario once or repeated for a time (timedloop), for a number of repetitions (loop) or forever. The results are stored and can be displayed by using “show logging diag-report”. Possible scenarios are “full” (all test purposes except the destructive ones), “quickturn” (scenarios running fast) or “write” (destructive scenarios).

**Format** `diagnostics interactive`  
`diagnostics <scenario> {{timedloop | loop} <1-9999999> | forever}`

**Mode** Privileged EXEC

### 5.13.2 show logging diag-report

This command displays the results of the last diagnostic run. The diagnostic results file is created by a diagnostic run..

**Format** `show logging diag-report`

**Mode** Privileged EXEC

## 5.14 PCI express Commands

### 5.14.1 show boardinfo pcie

This command displays the PCI Express clock settings.



- the kind of clock

**Format**            `show boardinfo pcie`

**Mode**             Privileged EXEC

## 5.15            Storage Commands

### 5.15.1        set board storage connect

This command sets the connection from an AMC to a storage modul. Possible connections are from AMC-B4 to AMC-B2 (port 2) or AMC-B1 (port 3).

**Format**            `set board storage connect amcb4 {amcb1|amcb2}`

**Mode**             Privileged EXEC

### 5.15.2        show boardinfo storage

This command displays the the connection from an AMC to a storage modul. Only connections from AMC-B4 are possible.

**Format**            `show boardinfo storage`

**Mode**             Privileged EXEC

## 5.16            Clock support commands

### 5.16.1        set board pcie clock

This command sets the kind of used clock. The clock can be a local SSC or local non-SSC.

**Format**            `set board pcie clock {ssc|nssc}`

**Mode**             Privileged EXEC

### 5.16.2        set board pll

This command sets the PLL configuration. Parameters are

- tie (time interval value: normal mode/adjust phase to match reference)
- mode (mode: normal operation/free run)
- oor (out-of-range select: 40 - 52 ppm/64 - 83 ppm)
- reset (reset: normal operation/reset)
- source (reference source: none/input CLK1A+B/input CLK2A+B/input CLK3A+B)



## Format

**Format**            `set board pll tie {normal|adjust}`  
                       `set board pll mode {normal|freerun}`  
                       `set board pll oor {40_52_ppm|64_83_ppm}`  
                       `set board pll reset {normal|reset}`  
                       `set board pll source {none|clk1|clk2|clk3}`

**Mode**             Priviledged EXEC

### 5.16.3            show boardinfo pll status

This command shows the PLL status.

**Format**            `show boardinfo pll status`

**Mode**             Priviledged EXEC

### 5.16.4            show boardinfo pll config

This command shows the PLL configuration. The PLL configuration parameters are described below for the “set” command.

**Format**            `show boardinfo pll config`

**Mode**             Priviledged EXEC

### 5.16.5            set board clock bpl

This command enables/disables a clock driver to the backplane.

**Format**            `set board clock bpl {clk1a|clk1b|clk2a|clk2b|clk3a|clk3b}`  
                       `{enable|disable}`

**Mode**             Priviledged EXEC

### 5.16.6            set board clock mux-amc

This command selects/deselects a source for a AMC clock (MUX configuration). The source may be the PLL (8kHz/19,44MHz auto selected by clock-ekeying), a backplane clock or another AMC clock. Default source is PLL. Settings are stored permamantly.

**Format**            `set board clock mux-amc {amcb1|amcb2|amcb3|amcb4} {tclka|tclkc} <src>`

**Mode**             Priviledged EXEC

<src>              = {pll|bpl<bplclk>|<amc>{tclkb|tclkd}}

<bplclk>           = {clk1a|clk1b|clk2a|clk2b|clk3a|clk3b}

### 5.16.7            set board clock mux-bpl

This command selects/deselects a source for a Backplane clock (MUX configuration). Default source is amcb1 tclkb. Settings are stored permanently.

**Format**            `set board clock mux-bpl <bplclk> {amcb1|amcb2|amcb3|amcb4} {tclkb|tclkd}`



**Mode** Privileged EXEC

<bplclk> = {clk1a|clk1b|clk2a|clk2b|clk3a|clk3b}

### 5.16.8 set board clock override

The command overrides the clock ekeying for an AMC clock. A correct MUX setting (set board clock mux-amc) must be done before. If the source for an AMC clock is set to PLL, the clock frequency must be specified too, otherwise the related parameter is not used.

**Format** **set board clock override** <amc> {tclka|tclkc} {enable|disable}  
[2kHz|8kHz|19\_44MHz]

**Mode** Privileged EXEC

<amc> = {amcb1|amcb2|amcb3|amcb4}

### 5.16.9 set board clock receiver

The command configures the clock description for clocks from the AMC. You can specify for family and accuracy either default values (sonet/stratum3 or sonet/stratum3E) or any protocol value (0..255). You can specify for frequency a well-known value or any other value (unit is Hz).

**Format** **set board clock receiver** <amc> {tclkb|tclkd} **enable** sonet  
{stratum3|stratum3E} {8kHz|1\_544MHz|2\_048\_MHz|19\_44MHz}  
**set board clock receiver** <amc> {tclkb|tclkd} **enable** <family> <accuracy>  
<frequency>  
**set board clock receiver** <amc> {tclkb|tclkd} **disable**

**Mode** Privileged EXEC

<amc> = {amcb1|amcb2|amcb3|amcb4}

### 5.16.10 set board clock source

The command configures the clock description for clocks to the AMC. You can specify for family and accuracy either default values (sonet/stratum3 or sonet/stratum3E) or any protocol value (0..255). You can specify for frequency a well-known value or any other value (unit is Hz).

**Format** **set board clock source** <amc> {tclka|tclkc} **enable** sonet  
{stratum3|stratum3E} {8kHz|1\_544MHz|2\_048\_MHz|19\_44MHz}  
**set board clock source** <amc> {tclka|tclkc} **enable** <family> <accuracy>  
{8kHz|1\_544MHz|2\_048\_MHz|19\_44MHz}  
**set board clock source** <amc> {tclka|tclkc} **disable**

**Mode** Privileged EXEC

<amc> = {amcb1|amcb2|amcb3|amcb4}

### 5.16.11 show boardinfo clock bpl

This command shows the configuration of backplane clocks. The backplane clocks are displayed with the state (enabled/disabled) and (if enabled) the mapped AMC source with clock configuration attributes.

**Format** **show boardinfo clock bpl**

**Mode** Privileged EXEC



### 5.16.12 show boardinfo clock amc

This command shows the configuration of the AMC clocks. The AMC clocks are displayed with the source (from carrier or AMC), state (enabled/disabled) and (if enabled) the internal clock index with clock configuration attributes. If the source is the AMC, it is checked whether a AMC is present (otherwise state is set to 'not present'). For source AMC the AMC is queried with the get clock state command and if the IPMI command is not supported the state is set to '--'. For source Carrier the clock state is queried from the local on-carrier device where the AMC clock is connected to.

**Format**            `show boardinfo clock amc`

**Mode**             Privileged EXEC







*Appendix*



---

# Getting Help

---



## A. Getting Help

If at any time you encounter difficulties with your application or with any of our products, or if you simply need guidance on system setups and capabilities, contact our Technical Support at:

### North America

Tel.: (450) 437-5682

Fax: (450) 437-8053

### EMEA

Tel.: +49 (0) 8341 803 xxx

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](http://www.kontron.com)

You also can contact us by E-mail at:

North America: [support@ca.kontron.com](mailto:support@ca.kontron.com)

EMEA: [support@kontron-modular.com](mailto:support@kontron-modular.com)

Or at the following address:

### North America

Kontron Canada, Inc.  
616 Curé Boivin  
Boisbriand, Québec  
J7G 2A7 Canada

### EMEA

Kontron Modular Computers GmbH  
Sudetenstrasse 7  
87600 Kaufbeuren  
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](mailto:RMA@ca.kontron.com) in North America and at [\\_\\_\\_\\_@\\_\\_\\_\\_.com](mailto:____@____.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

Kontron Canada, Inc.  
616 Curé Boivin  
Boisbriand, Québec  
J7G 2A7 Canada

### EMEA

Kontron Modular Computers GmbH  
Sudetenstrasse 7  
87600 Kaufbeuren  
Germany



**Return to  
Manufacturer  
Authorization Request**

Contact Name:	_____		
Company Name:	_____		
Street Address:	_____		
City:	_____	Province/State:	_____
Country:	_____	Postal/Zip Code:	_____
Phone Number:	_____	Extension:	_____
Fax Number:	_____	E-Mail:	_____

Serial Number	Failure or Problem Description	P.O. # (if not under warranty)

**Fax this form to Kontron's Technical Support department in North America at (450) 437-0304 and in EMEA at +49 (0)8341 803 XXX**





*Appendix*



---

# 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 intfNum(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 intfNum(x) unit x slot x port x	Interface creation out of order
NIM	NIM: L7_DELETE out of order for intfNum(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 intfNum(x)	A component responded with a fail indication for an interface event
NIM	NIM: Timeout event(x), intfNum(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)**

<b>Component</b>	<b>Message</b>	<b>Cause</b>
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**

<b>Component</b>	<b>Message</b>	<b>Cause</b>
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**

<b>Component</b>	<b>Message</b>	<b>Cause</b>
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

**Table 10: SNTP Log Message**

<b>Component</b>	<b>Message</b>	<b>Cause</b>
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**

<b>Component</b>	<b>Message</b>	<b>Cause</b>
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:rcvBufCnt 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	sshdApiCnfrCommand: 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	ssltApiCnfrCommand: 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 SSL certificate 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	protectedPortCnfrInitPhase1Process: Unable to create r/w lock for protectedPort	This appears when protectedPortCfgRWLock Fails
Protected Ports	protectedPortCnfrInitPhase2Process: 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 intfNum 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 intfNum 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	vlanIpSubnetCnfrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails
IPsubnet vlans	vlanIpSubnetCnfrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications
IPsubnet vlans	vlanIpSubnetCnfrFiniPhase1Process: 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	vlanMacCnfrInitPhase1Process: 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	vlanMacCnfrFiniPhase1Process: 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 a vlan delete notify event.

Table 20: 802.1x Log Messages

Component	Message	Cause
802.1X	<i>function</i> : Failed calling dot1xIssueCmd	802.1X message queue is full
802.1X	<i>function</i> : EAP message not received from server	RADIUS server did not send required EAP message
802.1X	<i>function</i> : Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers
802.1X	<i>function</i> : 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	<i>function</i> : failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server

Table 21: IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	<i>function</i> : 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	snoopCnfrgInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets
IGMP Snooping	snoopCnfrgInitPhase1Process: 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, garpApiCnfrCommand, 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	garpMapIntflsConfigurable, gmrpMapIntflsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntflsConfigurable.	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	dvlantagIntflsConfigurable: 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	ipv6ProvIntflsConfigurable: 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	dot1qMapIntflsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntflsConfigurable.	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	pmlMapIntflsConfigurable: Error accessing PML config data for interface %d in pmlMapIntflsConfigurable.	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 <i>name</i> , 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 <i>number</i>	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL <i>number</i> : 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, intfNum 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)*

<b>Component</b>	<b>Message</b>	<b>Cause</b>
<b>OSAPI Linux</b>	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**

---

# List of Commands

---

## C. List of Commands

{deny   permit} (IP ACL) .....	3 - 32
{deny   permit} (IPv6) .....	3 - 36
{deny   permit} (MAC ACL) .....	3 - 27
access-list .....	3 - 30
acl-trapflags .....	3 - 33
acl-traptimer .....	3 - 34
addport .....	2 - 61
advertise speed .....	2 - 3
arp access-list .....	2 - 90
assert (filter) .....	5 - 31
assign-queue .....	3 - 17
authentication login .....	2 - 41
authorization network radius .....	5 - 32
auto-negotiate .....	2 - 3
auto-negotiate all .....	2 - 3
auto-voip .....	3 - 39
auto-voip all .....	3 - 38
block .....	2 - 4
boot system .....	4 - 3
bootfile .....	4 - 38
bridge aging-time .....	2 - 130
cablestatus .....	4 - 58
class .....	3 - 18
class-map .....	3 - 10
class-map rename .....	3 - 10
classofservice dot1p-mapping .....	3 - 2
classofservice ip-dscp-mapping .....	3 - 3
classofservice trust .....	3 - 3
clear board event-log .....	4 - 24
clear config .....	4 - 26
clear counters .....	4 - 26
clear dot1x statistics .....	2 - 42
clear errcounter .....	4 - 24
clear host .....	4 - 49
clear igmpsnooping .....	4 - 26
clear ip arp inspection statistics .....	2 - 92
clear ip dhcp binding .....	4 - 42
clear ip dhcp conflict .....	4 - 43
clear ip dhcp server statistics .....	4 - 42
clear ip dhcp snooping binding .....	2 - 86
clear ip dhcp snooping statistics .....	2 - 86
clear isdp counters .....	2 - 133
clear isdp table .....	2 - 133
clear lldp remote-data .....	2 - 116
clear lldp statistics .....	2 - 116

clear pass .....	4 - 26
clear port-channel .....	4 - 27
clear radius statistics .....	2 - 42
clear traplog .....	4 - 27
clear vlan .....	4 - 27
client-identifier .....	4 - 36
client-name .....	4 - 36
configuration .....	5 - 6
conform-color .....	3 - 18
copy .....	4 - 29
copy (pre-login banner) .....	5 - 47
cos-queue min-bandwidth .....	3 - 3
cos-queue strict .....	3 - 4
crypto certificate generate .....	5 - 13
crypto key generate dsa .....	5 - 14
crypto key generate rsa .....	5 - 13
debug arp .....	4 - 50
debug auto-voip .....	4 - 50
debug clear .....	4 - 51
debug console .....	4 - 51
debug dot1x packet .....	4 - 51
debug igmpsnooping packet .....	4 - 51
debug igmpsnooping packet receive .....	4 - 53
debug igmpsnooping packet transmit .....	4 - 52
debug ip acl .....	4 - 53
debug ip igmp packet .....	4 - 54
debug ip mcache packet .....	4 - 54
debug isdp packet .....	2 - 136
debug lacp packet .....	4 - 54
debug mldsnooping packet .....	4 - 55
debug ping packet .....	4 - 55
debug sflow packet .....	4 - 56
debug spanning-tree bpdu .....	4 - 56
debug spanning-tree bpdu receive .....	4 - 57
debug spanning-tree bpdu transmit .....	4 - 57
default-router .....	4 - 36
delete .....	4 - 3
delete nvram:extra-profile .....	4 - 31
deleteport (Global Config) .....	2 - 62
deleteport (Interface Config) .....	2 - 62
description .....	2 - 4
diagnostics .....	5 - 47
diffserv .....	3 - 9
disable (filter) .....	5 - 31
disconnect .....	5 - 14
dns-server .....	4 - 37





domain-name .....	4 - 39
dos-control all .....	2 - 127
dos-control firstfrag .....	2 - 127
dos-control icmp .....	2 - 129
dos-control l4port .....	2 - 129
dos-control sipdip .....	2 - 127
dos-control tcpflag .....	2 - 128
dos-control tcpfrag .....	2 - 128
dot1x default-login .....	2 - 42
dot1x guest-vlan .....	2 - 43
dot1x initialize .....	2 - 43
dot1x login .....	2 - 43
dot1x max-req .....	2 - 43
dot1x max-users .....	2 - 44
dot1x port-control .....	2 - 44
dot1x port-control all .....	2 - 44
dot1x re-authenticate .....	2 - 45
dot1x re-authentication .....	2 - 45
dot1x system-auth-control .....	2 - 45
dot1x timeout .....	2 - 46
dot1x unauthenticated-vlan .....	2 - 47
dot1x user .....	2 - 47
download amcipmifw .....	4 - 2
download ipmifw .....	4 - 2
drop .....	3 - 17
dvlan-tunnel ethertype .....	2 - 30
ekeying (interface) .....	4 - 4
ekeying all (configure) .....	4 - 4
enable (filter) .....	5 - 31
enable (Privileged EXEC access) .....	5 - 2
enable passwd .....	4 - 27
enable passwd encrypted <password> .....	4 - 27
filedescr .....	4 - 3
hardware-address .....	4 - 37
host .....	4 - 37
interface .....	2 - 3
ip access-group .....	3 - 33
ip access-list .....	3 - 31
ip access-list rename .....	3 - 32
ip arp inspection filter .....	2 - 90
ip arp inspection limit .....	2 - 89
ip arp inspection trust .....	2 - 89
ip arp inspection validate .....	2 - 88
ip arp inspection vlan .....	2 - 88
ip arp inspection vlan logging .....	2 - 88
ip dhcp bootp automatic .....	4 - 42

ip dhcp conflict logging .....	4 - 42
ip dhcp excluded-address .....	4 - 41
ip dhcp filtering .....	4 - 45
ip dhcp filtering trust .....	4 - 46
ip dhcp ping packets .....	4 - 41
ip dhcp pool .....	4 - 35
ip dhcp snooping .....	2 - 80
ip dhcp snooping binding .....	2 - 82
ip dhcp snooping database .....	2 - 81
ip dhcp snooping database write-delay .....	2 - 81
ip dhcp snooping limit .....	2 - 82
ip dhcp snooping log-invalid .....	2 - 83
ip dhcp snooping trust .....	2 - 83
ip dhcp snooping verify mac-address .....	2 - 81
ip dhcp snooping vlan .....	2 - 80
ip domain list .....	4 - 47
ip domain lookup .....	4 - 46
ip domain name .....	4 - 47
ip domain retry .....	4 - 48
ip domain timeout .....	4 - 48
ip host .....	4 - 48
ip name server .....	4 - 47
ip ssh .....	5 - 11
ip ssh protocol .....	5 - 11
ip ssh server enable .....	5 - 11
ip telnet server enable .....	5 - 7
ip verify binding .....	2 - 82
ip verify source .....	2 - 83
ipmb (filter) .....	5 - 31
ipv6 access-list .....	3 - 35
ipv6 access-list rename .....	3 - 36
ipv6 traffic-filter .....	3 - 37
isdpa advertise-v2 .....	2 - 132
isdpa enable .....	2 - 132
isdpa holdtime .....	2 - 132
isdpa run .....	2 - 131
isdpa timer .....	2 - 132
key .....	5 - 44
L2-port-bridge .....	2 - 138
l2p actor admin .....	2 - 63
l2p actor admin key .....	2 - 63
l2p actor admin state .....	2 - 63
l2p actor admin state individual .....	2 - 64
l2p actor admin state longtimeout .....	2 - 64
l2p actor admin state passive .....	2 - 65
l2p actor port .....	2 - 65



lACP actor port priority .....	2 - 65
lACP actor system priority .....	2 - 65
lACP admin key .....	2 - 62
lACP collector max-delay .....	2 - 62
lACP partner admin key .....	2 - 66
lACP partner admin state .....	2 - 66
lACP partner admin state individual .....	2 - 67
lACP partner admin state longtimeout .....	2 - 67
lACP partner admin state passive .....	2 - 67
lACP partner port id .....	2 - 68
lACP partner port priority .....	2 - 68
lACP partner system priority .....	2 - 69
lACP partner system-id .....	2 - 69
lease .....	4 - 38
lineconfig .....	5 - 6
lldp med .....	2 - 120
lldp med all .....	2 - 122
lldp med confignotification .....	2 - 121
lldp med confignotification all .....	2 - 122
lldp med faststartrepeatcount .....	2 - 122
lldp med transmit-tlv .....	2 - 121
lldp med transmit-tlv all .....	2 - 122
lldp notification .....	2 - 115
lldp notification-interval .....	2 - 116
lldp receive .....	2 - 114
lldp timers .....	2 - 114
lldp transmit .....	2 - 113
lldp transmit-mgmt .....	2 - 115
lldp transmit-tlv .....	2 - 114
logging buffered .....	4 - 20
logging buffered wrap .....	4 - 20
logging cli-command .....	4 - 20
logging console .....	4 - 21
logging host .....	4 - 21
logging host remove .....	4 - 21
logging persistent .....	4 - 58
logging port .....	4 - 22
logging syslog .....	4 - 22
logout .....	4 - 27
mac access-group .....	3 - 29
mac access-list extended .....	3 - 27
mac access-list extended rename .....	3 - 27
macfilter .....	2 - 77
macfilter adddest .....	2 - 78
macfilter adddest all .....	2 - 78
macfilter addsrc .....	2 - 78

macfilter addsrc all .....	2 - 79
mark cos .....	3 - 19
mark ip-precedence .....	3 - 19
match any .....	3 - 11
match class-map .....	3 - 11
match cos .....	3 - 12
match destination-address mac .....	3 - 12
match dstip .....	3 - 13
match dstip6 .....	3 - 13
match dstl4port .....	3 - 13
match ethertype .....	3 - 10
match ip dscp .....	3 - 13
match ip precedence .....	3 - 14
match ip tos .....	3 - 14
match protocol .....	3 - 15
match secondary-cos .....	3 - 12
match secondary-vlan .....	3 - 16
match source-address mac .....	3 - 15
match srcip .....	3 - 15
match srcip6 .....	3 - 16
match srcl4port .....	3 - 16
match vlan .....	3 - 16
mirror .....	3 - 17
mode dot1q-tunnel .....	2 - 31
mode dvlan-tunnel .....	2 - 31
monitor session .....	2 - 75
mtu .....	2 - 4
multicast (interface) .....	2 - 136
multicast (VLAN) .....	2 - 137
netbios-name-server .....	4 - 39
netbios-node-type .....	4 - 39
network (DHCP Pool Config) .....	4 - 38
network mac-address .....	5 - 3
network mac-type .....	5 - 4
network mgmt_vlan .....	2 - 21
network parms .....	5 - 3
network protocol .....	5 - 3
next-server .....	4 - 40
no access-list.....	3 - 31
no acl-trapflags.....	3 - 33
no acl-traptimer .....	3 - 34
no advertise speed.....	2 - 4
no arp access-list.....	2 - 90
no authentication login .....	2 - 42
no authorization network radius .....	5 - 32
no auto-negotiate all .....	2 - 3



no auto-negotiate.....	2 - 3
no auto-voip all .....	3 - 38
no auto-voip .....	3 - 39
no block.....	2 - 4
no bootfile .....	4 - 39
no bridge aging-time .....	2 - 130
no class.....	3 - 19
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.....	4 - 36
no client-name.....	4 - 36
no cos-queue min-bandwidth .....	3 - 4
no cos-queue strict .....	3 - 4
no crypto certificate generate .....	5 - 13
no crypto key generate dsa.....	5 - 14
no crypto key generate rsa .....	5 - 13
no debug arp.....	4 - 50
no debug auto-voip .....	4 - 50
no debug console.....	4 - 51
no debug dot1x packet .....	4 - 51
no debug igmpsnooping packet .....	4 - 52
no debug igmpsnooping receive .....	4 - 53
no debug igmpsnooping transmit.....	4 - 52
no debug ip acl.....	4 - 54
no debug ip igmp packet .....	4 - 54
no debug ip mcache packet .....	4 - 54
no debug isdp packet.....	2 - 136
no debug lacp packet.....	4 - 55
no debug mldsnooping packet .....	4 - 55
no debug ping packet .....	4 - 56
no debug sflow packet .....	4 - 56
no debug spanning-tree bpdu receive .....	4 - 57
no debug spanning-tree bpdu transmit.....	4 - 58
no debug spanning-tree bpdu .....	4 - 56
no default-router.....	4 - 37
no diffserv .....	3 - 9
no dns-server.....	4 - 37
no domain-name.....	4 - 39
no dos-control all .....	2 - 127
no dos-control firstfrag .....	2 - 128
no dos-control icmp .....	2 - 129
no dos-control l4port.....	2 - 129
no dos-control sipdip.....	2 - 127
no dos-control tcpflag .....	2 - 128

no dos-control tcpfrag.....	2 - 128
no dot1x guest-vlan.....	2 - 43
no dot1x max-req.....	2 - 44
no dot1x max-users.....	2 - 44
no dot1x port-control all.....	2 - 45
no dot1x port-control.....	2 - 44
no dot1x re-authentication.....	2 - 45
no dot1x system-auth-control.....	2 - 46
no dot1x timeout.....	2 - 46
no dot1x unauthenticated-vlan.....	2 - 47
no dot1x user.....	2 - 47
no ekeying (interface).....	4 - 4
no ekeying all (configure).....	4 - 5
no hardware-address.....	4 - 37
no host.....	4 - 38
no ip access-group.....	3 - 33
no ip access-list.....	3 - 32
no ip arp inspection filter.....	2 - 90
no ip arp inspection limit.....	2 - 89
no ip arp inspection trust.....	2 - 89
no ip arp inspection validate.....	2 - 88
no ip arp inspection vlan logging.....	2 - 89
no ip arp inspection vlan.....	2 - 88
no ip dhcp bootp automatic.....	4 - 42
no ip dhcp conflict logging.....	4 - 42
no ip dhcp excluded-address.....	4 - 41
no ip dhcp filtering trust.....	4 - 46
no ip dhcp filtering.....	4 - 45
no ip dhcp ping packets.....	4 - 41
no ip dhcp pool.....	4 - 36
no ip dhcp snooping binding.....	2 - 82
no ip dhcp snooping database write-delay.....	2 - 81
no ip dhcp snooping limit.....	2 - 82
no ip dhcp snooping log-invalid.....	2 - 83
no ip dhcp snooping trust.....	2 - 83
no ip dhcp snooping verify mac-address.....	2 - 81
no ip dhcp snooping vlan.....	2 - 81
no ip dhcp snooping.....	2 - 80
no ip domain list.....	4 - 47
no ip domain lookup.....	4 - 46
no ip domain name.....	4 - 47
no ip domain retry.....	4 - 48
no ip domain timeout.....	4 - 49
no ip host.....	4 - 48
no ip name server.....	4 - 48
no ip ssh server enable.....	5 - 11

no ip telnet server enable .....	5 - 7
no ip verify binding .....	2 - 82
no ip verify source .....	2 - 83
no ipv6 access-list .....	3 - 36
no ipv6 traffic-filter .....	3 - 37
no isdp advertise-v2 .....	2 - 132
no isdp enable .....	2 - 133
no isdp run .....	2 - 132
no L2-port-bridge .....	2 - 138
no lacp actor admin key .....	2 - 63
no lacp actor admin state individual .....	2 - 64
no lacp actor admin state longtimeout .....	2 - 64
no lacp actor admin state passive .....	2 - 65
no lacp actor admin state .....	2 - 64
no lacp actor port priority .....	2 - 65
no lacp actor system priority .....	2 - 66
no lacp admin key .....	2 - 62
no lacp collector max delay .....	2 - 63
no lacp partner admin key .....	2 - 66
no lacp partner admin state individual .....	2 - 67
no lacp partner admin state longtimeout .....	2 - 67
no lacp partner admin state passive .....	2 - 68
no lacp partner admin state .....	2 - 66
no lacp partner port id .....	2 - 68
no lacp partner port priority .....	2 - 68
no lacp partner system priority .....	2 - 69
no lacp partner system-id .....	2 - 69
no ldp med confignotification .....	2 - 121
no lease .....	4 - 38
no lldp med faststartrepeatcount .....	2 - 122
no lldp med transmit-tlv .....	2 - 121
no lldp med transmit-tlv .....	2 - 123
no lldp med .....	2 - 121
no lldp notification .....	2 - 115
no lldp notification-interval .....	2 - 116
no lldp receive .....	2 - 114
no lldp timers .....	2 - 114
no lldp transmit .....	2 - 114
no lldp transmit-mgmt .....	2 - 115
no lldp transmit-tlv .....	2 - 115
no logging buffered wrap .....	4 - 20
no logging buffered .....	4 - 20
no logging cli-command .....	4 - 21
no logging console .....	4 - 21
no logging persistent .....	4 - 58
no logging port .....	4 - 22

no logging syslog.....	4 - 22
no mac access-group.....	3 - 29
no mac access-list extended.....	3 - 27
no macfilter adddest all .....	2 - 78
no macfilter adddest .....	2 - 78
no macfilter addsrc all .....	2 - 79
no macfilter addsrc .....	2 - 79
no macfilter.....	2 - 77
no match class-map .....	3 - 12
no mode dot1q-tunnel.....	2 - 31
no mode dvlan-tunnel .....	2 - 31
no monitor .....	2 - 76
no monitor session.....	2 - 76
no mtu.....	2 - 5
no netbios-name-server .....	4 - 39
no netbios-node-type .....	4 - 40
no network mac-type .....	5 - 4
no network mgmt_vlan.....	2 - 21
no network.....	4 - 38
no next-server .....	4 - 40
no option.....	4 - 40
no passwords aging.....	5 - 19
no passwords history .....	5 - 19
no passwords lock-out .....	5 - 20
no passwords min-length.....	5 - 19
no permit ip host mac host.....	2 - 90
no policy-map.....	3 - 20
no port lacpmode all .....	2 - 70
no port lacpmode .....	2 - 70
no port lacptimeout.....	2 - 71
no port lacptimeout.....	2 - 71
no port-channel adminmode .....	2 - 71
no port-channel linktrap .....	2 - 72
no port-channel load-balance .....	2 - 73
no port-channel static .....	2 - 70
no port-channel system priority.....	2 - 73
no port-channel.....	2 - 61
no port-security mac-address.....	2 - 112
no port-security max-dynamic.....	2 - 111
no port-security max-static .....	2 - 112
no port-security.....	2 - 111
no protection-group (configure) .....	3 - 8
no protection-group (interface).....	3 - 8
no protocol group .....	2 - 26
no protocol vlan group all.....	2 - 27
no protocol vlan group.....	2 - 26





no radius accounting mode .....	5 - 32
no radius server attribute.....	5 - 33
no radius server host .....	5 - 34
no radius server msgauth .....	5 - 35
no radius server retransmit.....	5 - 36
no radius server timeout.....	5 - 36
no serial baudrate .....	5 - 6
no serial timeout.....	5 - 6
no service dhcp .....	4 - 41
no service-policy.....	3 - 21
no session-limit .....	5 - 9
no session-timeout .....	5 - 9
no set board snmp ipmi-trap filter.....	5 - 30
no set board snmp site.....	5 - 30
no set bootstopkey.....	4 - 31
no set garp timer join .....	2 - 37
no set garp timer leave .....	2 - 37
no set garp timer leaveall .....	2 - 37
no set gmrp adminmode.....	2 - 40
no set gmrp interfacemode.....	2 - 40
no set groupmembership-interval .....	2 - 104
no set gvrp adminmode .....	2 - 38
no set gvrp interfacemode .....	2 - 39
no set igmp fast-leave .....	2 - 95
no set igmp groupmembership-interval .....	2 - 95
no set igmp interfacemode .....	2 - 94
no set igmp maxresponse .....	2 - 96
no set igmp mcrtexpiretime .....	2 - 97
no set igmp mrouter interface .....	2 - 97
no set igmp mrouter .....	2 - 97
no set igmp proxy-report interfacemode.....	2 - 137
no set igmp querier election participate .....	2 - 101
no set igmp querier query-interval .....	2 - 100
no set igmp querier timer expiry .....	2 - 101
no set igmp querier version.....	2 - 101
no set igmp querier.....	2 - 100
no set igmp.....	2 - 94
no set mld fast-leave .....	2 - 104
no set mld interfacemode .....	2 - 103
no set mld maxresponse .....	2 - 105
no set mld mcrtexpiretime .....	2 - 105
no set mld mrouter interface .....	2 - 106
no set mld mrouter .....	2 - 106
no set mld querier election participate .....	2 - 109
no set mld querier query_interval .....	2 - 109
no set mld querier timer expiry .....	2 - 109

no set mld querier .....	2 - 108
no set mld .....	2 - 103
no sflow poller .....	4 - 61
no sflow receiver .....	4 - 60
no sflow sampler .....	4 - 60
no shutdown all .....	2 - 5
no shutdown .....	2 - 5
no snmp trap link-status all .....	5 - 27
no snmp trap link-status .....	5 - 27
no snmp-server community ipaddr .....	5 - 21
no snmp-server community ipmask .....	5 - 22
no snmp-server community mode .....	5 - 22
no snmp-server community .....	5 - 21
no snmp-server enable traps linkmode .....	5 - 24
no snmp-server enable traps multiusers .....	5 - 24
no snmp-server enable traps pll .....	5 - 24
no snmp-server enable traps stpmode .....	5 - 25
no snmp-server enable traps violation .....	5 - 23
no snmp-server enable traps .....	5 - 23
no snmptrap mode .....	5 - 26
no snmptrap .....	5 - 25
no snmp broadcast client poll-interval .....	4 - 32
no snmp client mode .....	4 - 32
no snmp client port .....	4 - 32
no snmp server .....	4 - 34
no snmp unicast client poll-interval .....	4 - 33
no snmp unicast client poll-retry .....	4 - 33
no snmp unicast client poll-timeout .....	4 - 33
no spanning-tree bpdufilter default .....	2 - 8
no spanning-tree bpdufilter .....	2 - 8
no spanning-tree bpduflood .....	2 - 8
no spanning-tree bpduguard .....	2 - 9
no spanning-tree configuration name .....	2 - 9
no spanning-tree configuration revision .....	2 - 10
no spanning-tree edgeport .....	2 - 10
no spanning-tree forceversion .....	2 - 10
no spanning-tree forward-time .....	2 - 11
no spanning-tree hello-time .....	2 - 11
no spanning-tree max-age .....	2 - 11
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 rootguard .....	2 - 15
no spanning-tree .....	2 - 7
no sshcon maxsessions .....	5 - 12
no sshcon timeout .....	5 - 12
no storm-control broadcast all level .....	2 - 54
no storm-control broadcast all rate .....	2 - 54
no storm-control broadcast all .....	2 - 53
no storm-control broadcast level .....	2 - 53
no storm-control broadcast rate .....	2 - 53
no storm-control broadcast .....	2 - 52
no storm-control flowcontrol .....	2 - 59
no storm-control multicast all level .....	2 - 56
no storm-control multicast all rate .....	2 - 57
no storm-control multicast all .....	2 - 56
no storm-control multicast level .....	2 - 55
no storm-control multicast rate .....	2 - 55
no storm-control multicast .....	2 - 55
no storm-control unicast all level .....	2 - 59
no storm-control unicast all rate .....	2 - 59
no storm-control unicast all .....	2 - 58
no storm-control unicast level .....	2 - 57
no storm-control unicast .....	2 - 57
no storm-control unicast rate .....	2 - 58
no switchport protected (Global Config) .....	2 - 35
no switchport protected (Interface Config) .....	2 - 35
no tacacs-server host .....	5 - 43
no tacacs-server key .....	5 - 43
no tacacs-server timeout .....	5 - 43
no telnetcon maxsessions .....	5 - 9
no telnetcon timeout .....	5 - 10
no terminal length .....	4 - 17
no traffic-shape .....	3 - 4
no transport input telnet .....	5 - 8
no transport output telnet .....	5 - 8
no users name .....	5 - 15
no users passwd .....	5 - 16
no users snmpv3 accessmode .....	5 - 16
no users snmpv3 authentication .....	5 - 17
no users snmpv3 encryption .....	5 - 17
no vlan acceptframe .....	2 - 21
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 tagging .....	2 - 27
no vlan .....	2 - 21
no voice vlan (Global Config).....	2 - 33
no voice vlan (Interface Config).....	2 - 33
option .....	4 - 40
packet-memory (configure) .....	3 - 7
packet-memory (interface) .....	3 - 7
passwd .....	5 - 18
passwords aging .....	5 - 19
passwords history .....	5 - 19
passwords lock-out .....	5 - 20
passwords min-length .....	5 - 19
permit ip host mac host .....	2 - 90
ping .....	4 - 28
police-simple .....	3 - 20
policy-map .....	3 - 20
policy-map rename .....	3 - 21
port .....	5 - 44
port lacpmode .....	2 - 70
port lacpmode all .....	2 - 70
port lacptimeout (Global Config) .....	2 - 71
port lacptimeout (Interface Config) .....	2 - 70
port-channel .....	2 - 61
port-channel adminmode .....	2 - 71
port-channel hash multicast .....	2 - 73
port-channel linktrap .....	2 - 72
port-channel load-balance .....	2 - 72
port-channel name .....	2 - 73
port-channel static .....	2 - 69
port-channel system priority .....	2 - 73
port-security .....	2 - 111
port-security mac-address .....	2 - 112
port-security mac-address move .....	2 - 112
port-security max-dynamic .....	2 - 111
port-security max-static .....	2 - 111
priority .....	5 - 44
protection-group (configure) .....	3 - 7
protection-group (interface) .....	3 - 8
protocol group .....	2 - 26
protocol vlan group .....	2 - 26
protocol vlan group all .....	2 - 26
quit .....	4 - 29



radius accounting mode .....	5 - 32
radius server attribute .....	5 - 32
radius server host .....	5 - 33
radius server key .....	5 - 34
radius server msgauth .....	5 - 35
radius server primary .....	5 - 35
radius server retransmit .....	5 - 36
radius server timeout .....	5 - 36
redirect .....	3 - 18
reload .....	4 - 29
reload fast .....	4 - 29
script apply .....	5 - 46
script delete .....	5 - 46
script list .....	5 - 46
script show .....	5 - 46
script validate .....	5 - 46
serial baudrate .....	5 - 6
serial timeout .....	5 - 6
service dhcp .....	4 - 41
service-policy .....	3 - 21
serviceport ip .....	5 - 2
serviceport protocol .....	5 - 3
session-limit .....	5 - 9
session-timeout .....	5 - 9
set board clock bpl .....	5 - 49
set board clock mux-amc .....	5 - 49
set board clock mux-bpl .....	5 - 49
set board clock override .....	5 - 50
set board clock receiver .....	5 - 50
set board clock source .....	5 - 50
set board device-id .....	4 - 4
set board pcie clock .....	5 - 48
set board pll .....	5 - 48
set board sensor threshold .....	4 - 3
set board snmp ipmi-trap filter .....	5 - 30
set board snmp ipmi-trap interval .....	5 - 30
set board snmp ipmi-trap .....	5 - 30
set board snmp site .....	5 - 29
set board storage connect .....	5 - 48
set bootstopkey .....	4 - 31
set garp timer join .....	2 - 36
set garp timer leave .....	2 - 37
set garp timer leaveall .....	2 - 37
set gmrp adminmode .....	2 - 40
set gmrp interfacemode .....	2 - 40
set gvrp adminmode .....	2 - 38

set gvrp interfacemode .....	2 - 38
set igmp .....	2 - 93
set igmp fast-leave .....	2 - 95
set igmp groupmembership-interval .....	2 - 95
set igmp interfacemode .....	2 - 94
set igmp maxresponse .....	2 - 96
set igmp mcertexpiretime .....	2 - 96
set igmp mrouter .....	2 - 97
set igmp mrouter interface .....	2 - 97
set igmp proxy-report interfacemode .....	2 - 137
set igmp querier .....	2 - 100
set igmp querier election participate .....	2 - 101
set igmp querier query-interval .....	2 - 100
set igmp querier timer expiry .....	2 - 101
set igmp querier version .....	2 - 101
set mld .....	2 - 103
set mld fast-leave .....	2 - 104
set mld groupmembership-interval .....	2 - 104
set mld interfacemode .....	2 - 103
set mld maxresponse .....	2 - 105
set mld mcertexpiretime .....	2 - 105
set mld mrouter .....	2 - 105
set mld mrouter interface .....	2 - 106
set mld querier .....	2 - 108
set mld querier election participate .....	2 - 109
set mld querier query_interval .....	2 - 108
set mld querier timer expiry .....	2 - 109
set prompt .....	5 - 47
sflow poller .....	4 - 60
sflow receiver .....	4 - 59
sflow sampler .....	4 - 60
show access-lists .....	3 - 35
show acl-traptimer .....	3 - 34
show advertise speed .....	2 - 4
show arp access-list .....	2 - 93
show arp switch .....	4 - 5
show atca ekeying .....	4 - 4
show authentication .....	2 - 48
show authentication users .....	2 - 48
show auto-voip .....	3 - 39
show boardinfo address .....	4 - 18
show boardinfo amc connection .....	4 - 19
show boardinfo amc fru .....	4 - 19
show boardinfo amc ipmidev .....	4 - 19
show boardinfo clock amc .....	5 - 51
show boardinfo clock bpl .....	5 - 50

show boardinfo cpu-load .....	4 - 19
show boardinfo event-log .....	4 - 17
show boardinfo fru .....	4 - 18
show boardinfo ipmidev .....	4 - 19
show boardinfo led .....	4 - 19
show boardinfo memory-usage .....	4 - 20
show boardinfo pcie .....	5 - 47
show boardinfo pll config .....	5 - 49
show boardinfo pll status .....	5 - 49
show boardinfo post-status .....	4 - 17
show boardinfo sensors .....	4 - 17
show boardinfo snmp ipmi-trap .....	5 - 32
show boardinfo snmp site .....	5 - 30
show boardinfo storage .....	5 - 48
show boardinfo update-status .....	4 - 18
show boardinfo version .....	4 - 18
show bootvar .....	4 - 3
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 diffserv .....	3 - 23
show diffserv service .....	3 - 25
show diffserv service brief .....	3 - 25
show dos-control .....	2 - 129
show dot1q-tunnel .....	2 - 31
show dot1x .....	2 - 48
show dot1x clients .....	2 - 50
show dot1x users .....	2 - 51
show dvlan-tunnel .....	2 - 32
show eventlog .....	4 - 5
show forwardingdb agetime .....	2 - 130
show garp .....	2 - 38
show gmrp configuration .....	2 - 40
show gvrp configuration .....	2 - 39
show hardware .....	4 - 6
show hosts .....	4 - 49
show igmpsnooping .....	2 - 97
show igmpsnooping mrouter interface .....	2 - 98
show igmpsnooping mrouter vlan .....	2 - 99
show igmpsnooping querier .....	2 - 102
show interface .....	4 - 6
show interface cos-counter .....	3 - 6
show interface ethernet .....	4 - 7
show interfaces cos-queue .....	3 - 6

show interfaces switchport .....	2 - 36
show ip access-lists .....	3 - 34
show ip arp inspection .....	2 - 91
show ip arp inspection interfaces .....	2 - 92
show ip arp inspection statistics .....	2 - 91
show ip dhcp binding .....	4 - 43
show ip dhcp conflict .....	4 - 45
show ip dhcp filtering .....	4 - 46
show ip dhcp global configuration .....	4 - 43
show ip dhcp pool configuration .....	4 - 43
show ip dhcp server statistics .....	4 - 44
show ip dhcp snooping .....	2 - 84
show ip dhcp snooping binding .....	2 - 84
show ip dhcp snooping database .....	2 - 85
show ip dhcp snooping statistics .....	2 - 85
show ip source binding .....	2 - 87
show ip ssh .....	5 - 12
show ip verify source .....	2 - 86
show ipv6 access-lists .....	3 - 37
show isdp .....	2 - 133
show isdp entry .....	2 - 134
show isdp interface .....	2 - 134
show isdp neighbors .....	2 - 134
show isdp traffic .....	2 - 135
show lacp actor .....	2 - 73
show lacp partner .....	2 - 74
show lldp .....	2 - 116
show lldp interface .....	2 - 117
show lldp local-device .....	2 - 119
show lldp local-device detail .....	2 - 120
show lldp med .....	2 - 123
show lldp med interface .....	2 - 123
show lldp med local-device detail .....	2 - 124
show lldp med remote-device .....	2 - 125
show lldp med remote-device detail .....	2 - 125
show lldp remote-device .....	2 - 118
show lldp remote-device detail .....	2 - 118
show lldp statistics .....	2 - 117
show logging .....	4 - 22
show logging backtrace .....	4 - 24
show logging buffered .....	4 - 23
show logging diag-report .....	5 - 47
show logging errcounter .....	4 - 24
show logging hosts .....	4 - 23
show logging persistent .....	4 - 24
show logging traplogs .....	4 - 23



show loginsession .....	5 - 14
show mac access-lists .....	3 - 29
show mac-address-table gmrp .....	2 - 41
show mac-address-table igmpsnooping .....	2 - 99
show mac-address-table mldsnooping .....	2 - 107
show mac-address-table multicast .....	2 - 131
show mac-address-table static .....	2 - 79
show mac-address-table staticfiltering .....	2 - 80
show mac-address-table stats .....	2 - 131
show mac-addr-table .....	4 - 13
show mldsnooping .....	2 - 106
show mldsnooping mrouter interface .....	2 - 107
show mldsnooping mrouter vlan .....	2 - 107
show mldsnooping querier .....	2 - 110
show monitor session .....	2 - 76
show network .....	5 - 4
show packet-memory .....	3 - 6
show passwords configuration .....	5 - 20
show policy-map .....	3 - 23
show policy-map interface .....	3 - 25
show port .....	2 - 6
show port multicast .....	2 - 136
show port protocol .....	2 - 7
show port-channel .....	2 - 75
show port-channel brief .....	2 - 74
show port-channel hash multicast .....	2 - 75
show port-channel system priority .....	2 - 75
show port-security .....	2 - 112
show port-security dynamic .....	2 - 113
show port-security static .....	2 - 113
show port-security violation .....	2 - 113
show process cpu .....	4 - 14
show protection-group .....	3 - 7
show radius .....	5 - 36
show radius accounting .....	5 - 39
show radius accounting statistics .....	5 - 40
show radius servers .....	5 - 37
show radius statistics .....	5 - 41
show running-config .....	4 - 15
show serial .....	5 - 7
show service-policy .....	3 - 26
show serviceport .....	5 - 5
show sflow agent .....	4 - 61
show sflow receivers .....	4 - 62
show sflow samplers .....	4 - 62
show snmpcommunity .....	5 - 27

show snmp-engine-id .....	5 - 29
show snmptrap .....	5 - 28
show snmp .....	4 - 34
show snmp client .....	4 - 34
show snmp server .....	4 - 35
show spanning-tree .....	2 - 16
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 - 60
show switchport protected .....	2 - 36
show sysinfo .....	4 - 16
show tacacs .....	5 - 44
show tech-support .....	4 - 16
show telnet .....	5 - 10
show telnetcon .....	5 - 10
show terminal length .....	4 - 17
show trapflags .....	5 - 28
show users .....	5 - 18
show users accounts .....	5 - 18
show users authentication .....	2 - 51
show version .....	4 - 6
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 - 137
show vlan port .....	2 - 29
show voice vlan .....	2 - 33
shutdown .....	2 - 5
shutdown all .....	2 - 5
snmp trap link-status .....	5 - 26
snmp trap link-status all .....	5 - 27
snmp-server .....	5 - 21
snmp-server community .....	5 - 21
snmp-server community ipaddr .....	5 - 21
snmp-server community ipmask .....	5 - 22
snmp-server community mode .....	5 - 22
snmp-server community ro .....	5 - 22
snmp-server enable traps .....	5 - 23
snmp-server enable traps linkmode .....	5 - 24
snmp-server enable traps multiusers .....	5 - 24

snmp-server enable traps pll .....	5 - 24
snmp-server enable traps stpmode .....	5 - 25
snmp-server enable traps violation .....	5 - 23
snmp-server engine-id .....	5 - 29
snmptrap .....	5 - 25
snmptrap ipaddr .....	5 - 26
snmptrap mode .....	5 - 26
snmptrap notification .....	5 - 29
snmptrap snmpversion .....	5 - 26
sntp broadcast client poll-interval .....	4 - 32
sntp client mode .....	4 - 32
sntp client port .....	4 - 32
sntp server .....	4 - 34
sntp unicast client poll-interval .....	4 - 33
sntp unicast client poll-retry .....	4 - 33
sntp unicast client poll-timeout .....	4 - 33
spanning-tree .....	2 - 7
spanning-tree bpdudfilter .....	2 - 8
spanning-tree bpdudfilter 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 - 9
spanning-tree edgeport .....	2 - 10
spanning-tree forceversion .....	2 - 10
spanning-tree forward-time .....	2 - 11
spanning-tree hello-time .....	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 - 13
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
spanning-tree rootguard .....	2 - 15
speed .....	2 - 6
speed all .....	2 - 6
sshcon maxsessions .....	5 - 12
sshcon timeout .....	5 - 12
status (filter) .....	5 - 31
storm-control broadcast .....	2 - 52
storm-control broadcast all .....	2 - 53
storm-control broadcast all level .....	2 - 54

storm-control broadcast all rate .....	2 - 54
storm-control broadcast level .....	2 - 52
storm-control broadcast rate .....	2 - 53
storm-control flowcontrol .....	2 - 59
storm-control multicast .....	2 - 54
storm-control multicast all .....	2 - 56
storm-control multicast all level .....	2 - 56
storm-control multicast all rate .....	2 - 56
storm-control multicast level .....	2 - 55
storm-control multicast rate .....	2 - 55
storm-control unicast .....	2 - 57
storm-control unicast all .....	2 - 58
storm-control unicast all level .....	2 - 58
storm-control unicast all rate .....	2 - 59
storm-control unicast level .....	2 - 57
storm-control unicast rate .....	2 - 58
switchport protected (Global Config) .....	2 - 35
switchport protected (Interface Config) .....	2 - 35
tacacs-server host .....	5 - 42
tacacs-server key .....	5 - 43
tacacs-server timeout .....	5 - 43
telnet .....	5 - 7
telnetcon maxsessions .....	5 - 9
telnetcon timeout .....	5 - 10
terminal length .....	4 - 16
timeout .....	5 - 44
traceroute .....	4 - 25
traffic-shape .....	3 - 4
transport input telnet .....	5 - 8
transport output telnet .....	5 - 8
type (filter) .....	5 - 31
users defaultlogin .....	2 - 47
users login .....	2 - 47
users name .....	5 - 15
users name <username> unlock .....	5 - 15
users passwd .....	5 - 15
users passwd <username> encrypted <password> .....	5 - 16
users snmpv3 accessmode .....	5 - 16
users snmpv3 authentication .....	5 - 17
users snmpv3 encryption .....	5 - 17
vlan .....	2 - 21
vlan acceptframe .....	2 - 21
vlan association mac .....	2 - 28
vlan association subnet .....	2 - 27
vlan database .....	2 - 20
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 - 34
vlan port pvid all .....	2 - 24
vlan port tagging all .....	2 - 25
vlan priority .....	2 - 34
vlan protocol group .....	2 - 25
vlan protocol group add protocol .....	2 - 25
vlan protocol group remove .....	2 - 26
vlan pvid .....	2 - 27
vlan tagging .....	2 - 27
voice vlan (Global Config) .....	2 - 32
voice vlan (Interface Config) .....	2 - 33
voice vlan data priority .....	2 - 33
write memory .....	5 - 20