Disclaimer

Kontron would like to point out that the information contained in this manual may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the manual or any product characteristics set out in the manual. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this manual are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this manual only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

This manual is protected by copyright. All rights are reserved by Kontron. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron. Kontron points out that the information contained in this manual is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this manual only reflects the technical status of the products by Kontron at the time of publishing.

Brand and product names are trademarks or registered trademarks of their respective owners.

© 2013, 2014 by Kontron America, ©2016 by Kontron AG

Kontron AG
Lise-Meitner-Straße 3-5
86156 Augsburg
Germany
www.kontron.com
High Risk Applications Hazard Notice

THIS DEVICE AND ASSOCIATED SOFTWARE ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE FOR THE OPERATION OF NUCLEAR FACILITIES, THE NAVIGATION, CONTROL OR COMMUNICATION SYSTEMS FOR AIRCRAFT OR OTHER TRANSPORTATION, AIR TRAFFIC CONTROL, LIFE SUPPORT OR LIFE SUSTAINING APPLICATIONS, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION IN A HAZARDOUS ENVIRONMENT, OR REQUIRING FAIL-SAFE PERFORMANCE, OR IN WHICH THE FAILURE OF PRODUCTS COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE (COLLECTIVELY, “HIGH RISK APPLICATIONS”).

You understand and agree that your use of Kontron devices as a component in High Risk Applications is entirely at your risk. To minimize the risks associated with your products and applications, you should provide adequate design and operating safeguards. You are solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning your products. You are responsible to ensure that your systems (and any Kontron hardware or software components incorporated in your systems) meet all applicable requirements. Unless otherwise stated in the product documentation, the Kontron device is not provided with error-tolerance capabilities and cannot therefore be deemed as being engineered, manufactured or setup to be compliant for implementation or for resale as device in High Risk Applications. All application and safety related information in this document (including application descriptions, suggested safety measures, suggested Kontron products, and other materials) is provided for reference only.
## Revision History

<table>
<thead>
<tr>
<th>Rev. Index</th>
<th>Brief Description of Changes</th>
<th>Date of Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Issue</td>
<td>2017, April 12</td>
</tr>
</tbody>
</table>
Terms and Conditions

Kontron warrants products in accordance with defined regional warranty periods. For more information about warranty compliance and conformity, and the warranty period in your region, visit http://www.kontron.com/terms-and-conditions.


For contact information, refer to the corporate offices contact information on the last page of this user guide or visit our website CONTACT US.

Customer Support

Find Kontron contacts by visiting: http://www.kontron.com/support

Customer Service

As a trusted technology innovator and global solutions provider, Kontron extends its embedded market strengths into a services portfolio allowing companies to break the barriers of traditional product lifecycles. Proven product expertise coupled with collaborative and highly-experienced support enables Kontron to provide exceptional peace of mind to build and maintain successful products. For more details on Kontron’s service offerings such as: enhanced repair services, extended warranty, Kontron training academy, and more visit http://www.kontron.com/support-and-services/services.

Customer Comments

If you have any difficulties using this guide, discover an error, or just want to provide some feedback, please send a message to Kontron. Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised user guide on our website.
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.

This document assumes that the reader has a basic knowledge of Ethernet and networking concepts.

Please note, FASTPATH 8.x SW versions and higher are only running on boards, equipped with extended memory.

How to Use this Document
Chapter 1, “Using the Command-Line Interface” on page 15 details the procedure to quickly become acquainted with the FASTPATH software.

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.
Symbols

The following symbols may be used in this manual.

**DANGER** indicates a hazardous situation which, if not avoided, will result in death or serious injury.

**WARNING** indicates a hazardous situation which, if not avoided, could result in death or serious injury.

**CAUTION** indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.

**NOTICE** indicates a property damage message.

**Electric Shock!**

This symbol and title warn of hazards due to electrical shocks (> 60 V) 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 „High.Voltage Safety Instructions“ portion below in this section.

**ESD Sensitive Device!**

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

**HOT Surface!**

Do NOT touch! Allow to cool before servicing.

**General Information**

This symbol indicates general information about the product and the user manual.

This symbol also indicates detail information about the specific product configuration.

**Helpful Hints and Tips**

This symbol precedes helpful hints and tips for daily use.
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

As a precaution and in case of danger, the power connector must be easily accessible. The power connector is the product’s main disconnect device.

---

**Warning**

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

---

**Electric Shock!**

Before installing a non hot-swappable Kontron product into a system always ensure that your mains power is switched off. This also applies to the installation of piggybacks. Serious electrical shock hazards can exist during all installation, repair, and maintenance operations on this product. Therefore, always unplug the power cable and any other cables which provide external voltages before performing any work on this product. Earth ground connection to vehicle’s chassis or a central grounding point shall remain connected. The earth ground cable shall be the last cable to be disconnected or the first cable to be connected when performing installation or removal procedures on this product.

---

Special Handling and Unpacking Instruction

---

**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 backup, ensure that the product 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 product.
Lithium Battery Precautions

If your product is equipped with a lithium battery, take the following precautions when replacing the battery.

---

<table>
<thead>
<tr>
<th>CAUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Danger of explosion if the battery is replaced incorrectly.</td>
</tr>
<tr>
<td>• Replace only with same or equivalent battery type recommended by the manufacturer.</td>
</tr>
<tr>
<td>• Dispose of used batteries according to the manufacturer's instructions.</td>
</tr>
</tbody>
</table>

---

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 product, that are not explicitly approved by Kontron and described in this User Guide or received from Kontron's Technical Support as a special handling instruction, will void your warranty.

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

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

Keep all the original packaging material for future storage or warranty shipments. If it is necessary to store or ship the product then re-pack it in the same manner as it was delivered.

Special care is necessary when handling or unpacking the product. See Special Handling and Unpacking Instruction.

Quality and Environmental Management

Kontron aims to deliver reliable high-end products designed and built for quality, and aims to complying with environmental laws, regulations, and other environmentally oriented requirements. For more information regarding Kontron's quality and environmental responsibilities, visit http://www.kontron.com/about-kontron/corporate-responsibility/quality-management.

Disposal and Recycling

Kontron's products are manufactured to satisfy environmental protection requirements where possible. Many of the components used are capable of being recycled. Final disposal of this product after its service life must be accomplished in accordance with applicable country, state, or local laws or regulations.

WEEE Compliance

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to:

• Reduce waste arising from electrical and electronic equipment (EEE)
• Make producers of EEE responsible for the environmental impact of their products, especially when the product become waste
• Encourage separate collection and subsequent treatment, reuse, recovery, recycling and sound environmental disposal of EEE
• Improve the environmental performance of all those involved during the lifecycle of EEE.

Environmental protection is a high priority with Kontron.

Kontron follows the DEEE/WEEE directive

You are encouraged to return our products for proper disposal.
# Table of Contents

Disclaimer ................................................................................................................................. 2  
High Risk Applications Hazard Notice ................................................................................... 3  
Revision History .................................................................................................................... 4  
Terms and Conditions ........................................................................................................... 5  
Customer Support ............................................................................................................... 5  
Customer Service ............................................................................................................... 5  
Customer Comments ......................................................................................................... 5  

1/ Using the Command-Line Interface ...................................................................................... 14  
   1.1 Command Syntax ........................................................................................................... 14  
   1.2 Command Conventions ............................................................................................... 14  
   1.3 Common Parameter Values ......................................................................................... 15  
   1.4 Slot/Port Naming Convention ..................................................................................... 16  
   1.5 Using the "No" Form of a Command .......................................................................... 16  
   1.6 FASTPATH Modules .................................................................................................... 17  
   1.7 Command Modes ....................................................................................................... 17  
   1.8 Command Completion and Abbreviation ................................................................... 19  
   1.9 CLI Error Messages .................................................................................................... 19  
   1.10 CLI Line-Editing Conventions .................................................................................. 20  
   1.11 Using CLI Help ......................................................................................................... 20  
   1.12 Accessing the CLI .................................................................................................... 21  

2/ Management Commands .................................................................................................... 22  
   2.1 Network Interface Commands ....................................................................................... 22  
   2.2 Console Port Access Commands ................................................................................... 27  
   2.3 Telnet Commands ........................................................................................................ 29  
   2.4 Secure Shell Commands .............................................................................................. 33  
   2.5 Management Security Commands ............................................................................. 36  
   2.6 Hypertext Transfer Protocol Commands ..................................................................... 37  
   2.7 Access Commands ..................................................................................................... 45  
   2.8 User Account Commands ............................................................................................ 46  
   2.9 SNMP Commands ....................................................................................................... 71  
   2.10 RADIUS Commands ............................................................................................... 85  
   2.11 TACACS+ Commands ............................................................................................... 104  
   2.12 Configuration Scripting Commands .......................................................................... 109  
   2.13 Prelogin Banner, System Prompt, and Host Name Commands .................................... 111  

3/ Utility Commands .............................................................................................................. 113  
   3.1 AutoInstall Commands ............................................................................................... 114  
   3.2 CLI Output Filtering Commands .................................................................................. 116  
   3.3 Dual Image Commands ............................................................................................... 118  
   3.4 System Information and Statistics Commands ......................................................... 118  
   3.5 Logging Commands .................................................................................................... 140  
   3.6 Email Alerting and Mail Server Commands .............................................................. 147  
   3.7 System Utility and Clear Commands ........................................................................ 152  
   3.8 SFP handling Commands ........................................................................................... 167  

www.kontron.com
3.9  Commands to configure startup services ..................................................................................... 169
3.10  Simple Network Time Protocol Commands .................................................................................. 169
3.11  Time Zone Commands ..................................................................................................................... 174
3.12  DHCP Server Commands ................................................................................................................ 178
3.13  DNS Client Commands ................................................................................................................... 189
3.14  IP Address Conflict Commands ................................................................................................... 194
3.15  Serviceability Packet Tracing Commands ...................................................................................... 195
3.16  BCM Shell Command ...................................................................................................................... 236
3.17  Cable Test Command ....................................................................................................................... 237
3.18  sFlow Commands ............................................................................................................................ 237
3.19  Switch Database Management Template Commands ..................................................................... 246
3.20  Remote Monitoring Commands .................................................................................................... 249
3.21  Statistics Application Commands .................................................................................................. 263
3.22  Precision Time Protocol (IEEE 1588) Commands ......................................................................... 268
3.23  Power Over Ethernet Commands ................................................................................................ 281

4/ Switching Commands .......................................................................................................................... 289
4.1  Port Configuration Commands ......................................................................................................... 290
4.2  Spanning Tree Protocol Commands ................................................................................................. 298
4.3  Loop Protection Commands ............................................................................................................. 322
4.4  VLAN Commands .............................................................................................................................. 325
4.5  Double VLAN Commands ................................................................................................................. 336
4.6  Private VLAN Commands ................................................................................................................ 339
4.7  Switch Ports ...................................................................................................................................... 341
4.8  Voice VLAN Commands ................................................................................................................... 344
4.9  Provisioning (IEEE 802.1p) Commands ............................................................................................ 346
4.10  Asymmetric Flow Control ............................................................................................................... 347
4.11  Protected Ports Commands ............................................................................................................ 348
4.12  GARP Commands .......................................................................................................................... 350
4.13  GVRP Commands ........................................................................................................................... 351
4.14  GMRP Commands .......................................................................................................................... 353
4.15  Port-Based Network Access Control Commands .......................................................................... 355
4.16  802.1X Supplicant Commands ................................................................................................... 371
4.17  Storm-Control Commands ............................................................................................................. 374
4.18  Link Dependency Commands ........................................................................................................ 382
4.19  Link Local Protocol Filtering Commands ..................................................................................... 384
4.20  MVR Commands ............................................................................................................................ 385
4.21  Port-Channel/LAG (802.3ad) Commands ...................................................................................... 389
4.22  VPC Commands ............................................................................................................................. 407
4.23  Port Mirroring Commands ............................................................................................................. 418
4.24  Static MAC Filtering Commands .................................................................................................. 424
4.25  DHCP L2 Relay Agent Commands ............................................................................................... 427
4.26  DHCP Client Commands ................................................................................................................ 433
4.27  DHCP Snooping Configuration Commands ................................................................................... 435
4.28  Dynamic ARP Inspection Commands .......................................................................................... 443
4.29  IGMP Snooping Configuration Commands .................................................................................... 449
4.30  IGMP Snooping Querier Commands .............................................................................................. 457
4.31  MLD Snooping Commands ........................................................................................................... 460
4.32  MLD Snooping Querier Commands .............................................................................................. 468
4.33  Port Security Commands ............................................................................................................. 470
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.34</td>
<td>LLDP (802.1AB) Commands</td>
<td>474</td>
</tr>
<tr>
<td>4.35</td>
<td>LLDP-MED Commands</td>
<td>481</td>
</tr>
<tr>
<td>4.36</td>
<td>Denial of Service Commands</td>
<td>488</td>
</tr>
<tr>
<td>4.37</td>
<td>MAC Database Commands</td>
<td>498</td>
</tr>
<tr>
<td>4.38</td>
<td>ISDP Commands</td>
<td>499</td>
</tr>
<tr>
<td>4.39</td>
<td>Interface Error Disable and Auto Recovery</td>
<td>505</td>
</tr>
<tr>
<td>4.40</td>
<td>Port Bridging Commands</td>
<td>508</td>
</tr>
<tr>
<td>5.1</td>
<td>Address Resolution Protocol Command</td>
<td>509</td>
</tr>
<tr>
<td>5.2</td>
<td>IP Routing Commands</td>
<td>514</td>
</tr>
<tr>
<td>5.3</td>
<td>Routing Policy Commands</td>
<td>535</td>
</tr>
<tr>
<td>5.4</td>
<td>Router Discovery Protocol Commands</td>
<td>549</td>
</tr>
<tr>
<td>5.5</td>
<td>Virtual LAN Routing Commands</td>
<td>552</td>
</tr>
<tr>
<td>5.6</td>
<td>Virtual Router Redundancy Protocol Commands</td>
<td>555</td>
</tr>
<tr>
<td>5.7</td>
<td>VRRPv3 Commands</td>
<td>562</td>
</tr>
<tr>
<td>5.8</td>
<td>DHCP and BOOTP Relay Commands</td>
<td>573</td>
</tr>
<tr>
<td>5.9</td>
<td>IP Helper Commands</td>
<td>577</td>
</tr>
<tr>
<td>5.10</td>
<td>Open Shortest Path First Commands</td>
<td>583</td>
</tr>
<tr>
<td>5.11</td>
<td>Routing Information Protocol Commands</td>
<td>631</td>
</tr>
<tr>
<td>5.12</td>
<td>ICMP Throttling Commands</td>
<td>638</td>
</tr>
<tr>
<td>5.13</td>
<td>Bidirectional Forwarding Detection Commands</td>
<td>640</td>
</tr>
<tr>
<td>6.1</td>
<td>IPv6 Management Commands</td>
<td>644</td>
</tr>
<tr>
<td>6.2</td>
<td>Tunnel Interface Commands</td>
<td>650</td>
</tr>
<tr>
<td>6.3</td>
<td>Loopback Interface Commands</td>
<td>652</td>
</tr>
<tr>
<td>6.4</td>
<td>IPv6 Routing Commands</td>
<td>652</td>
</tr>
<tr>
<td>6.5</td>
<td>OSPFv3 Commands</td>
<td>680</td>
</tr>
<tr>
<td>6.6</td>
<td>DHCPv6 Commands</td>
<td>714</td>
</tr>
<tr>
<td>6.7</td>
<td>DHCPv6 Snooping Configuration Commands</td>
<td>723</td>
</tr>
<tr>
<td>7.1</td>
<td>Class of Service Commands</td>
<td>732</td>
</tr>
<tr>
<td>7.2</td>
<td>Differentiated Services Commands</td>
<td>742</td>
</tr>
<tr>
<td>7.3</td>
<td>DiffServ Class Commands</td>
<td>743</td>
</tr>
<tr>
<td>7.4</td>
<td>DiffServ Policy Commands</td>
<td>750</td>
</tr>
<tr>
<td>7.5</td>
<td>DiffServ Service Commands</td>
<td>756</td>
</tr>
<tr>
<td>7.6</td>
<td>DiffServ Show Commands</td>
<td>757</td>
</tr>
<tr>
<td>7.7</td>
<td>MAC Access Control List Commands</td>
<td>762</td>
</tr>
<tr>
<td>7.8</td>
<td>IP Access Control List Commands</td>
<td>769</td>
</tr>
<tr>
<td>7.9</td>
<td>IPv6 Access Control List Commands</td>
<td>784</td>
</tr>
<tr>
<td>7.10</td>
<td>Time Range Commands for Time-Based ACLs</td>
<td>792</td>
</tr>
<tr>
<td>7.11</td>
<td>Auto-Voice over IP Commands</td>
<td>794</td>
</tr>
<tr>
<td>7.12</td>
<td>iSCSI Optimization Commands</td>
<td>798</td>
</tr>
<tr>
<td>8.1</td>
<td>Multicast Commands</td>
<td>803</td>
</tr>
<tr>
<td>8.2</td>
<td>DVMRP Commands</td>
<td>812</td>
</tr>
</tbody>
</table>
8.3 PIM Commands .......................................................................................................................... 816
8.4 Internet Group Message Protocol Commands ............................................................................. 830
8.5 IGMP Proxy Commands .............................................................................................................. 837

9/ IPv6 Multicast Commands ........................................................................................................... 842
9.1 IPv6 Multicast Forwarder ............................................................................................................ 842
9.2 IPv6 PIM Commands .................................................................................................................... 845
9.3 IPv6 MLD Commands .................................................................................................................. 857
9.4 IPv6 MLD-Proxy Commands ...................................................................................................... 862

10/ FASTPATH Log Messages ......................................................................................................... 867
10.1 Core ........................................................................................................................................ 867
10.2 Utilities .................................................................................................................................. 869
10.3 Management ............................................................................................................................. 872
10.4 Switching ................................................................................................................................. 876
10.5 QoS ........................................................................................................................................ 876
10.6 Routing/IPv6 Routing ................................................................................................................ 884
10.7 Multicast ................................................................................................................................... 887
10.8 Technologies ............................................................................................................................ 892
10.9 O/S Support ............................................................................................................................. 894

APPENDIX A: ...................................................................................................................... List of Commands 896
1/ Using the Command-Line Interface

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

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

- “Command Syntax” on page 14
- “Command Conventions” on page 14
- “Common Parameter Values” on page 15
- “Slot/Port Naming Convention” on page 16
- “Using the “No” Form of a Command” on page 16
- “FASTPATH Modules” on page 17
- “Command Modes” on page 17
- “Command Completion and Abbreviation” on page 19
- “CLI Error Messages” on page 19
- “CLI Line-Editing Conventions” on page 20
- “Using CLI Help” on page 20
- “Accessing the CLI” on page 21

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.
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.

The following table describes common parameter values and value formatting.

Table 1: Parameter Conventions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&gt; angle brackets</td>
<td>&lt;value&gt;</td>
<td>Indicates that you must enter a value in place of the brackets and text inside them.</td>
</tr>
<tr>
<td>[] square brackets</td>
<td>[value]</td>
<td>Indicates an optional parameter that you can enter in place of the brackets and text inside them.</td>
</tr>
<tr>
<td>{} curly braces</td>
<td>{choice1</td>
<td>choice2}</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>choice1</td>
</tr>
<tr>
<td></td>
<td>Braces within square brackets</td>
<td>{[choice1</td>
</tr>
</tbody>
</table>

Table 2: Parameter Descriptions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>This parameter is a valid IP address. You can enter the IP address in the following formats:</td>
</tr>
<tr>
<td></td>
<td>a (32 bits)</td>
</tr>
<tr>
<td></td>
<td>a.b (8.24 bits)</td>
</tr>
<tr>
<td></td>
<td>a.b.c (8.8.16 bits)</td>
</tr>
<tr>
<td></td>
<td>a.b.c.d (8.8.8.8)</td>
</tr>
<tr>
<td></td>
<td>In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where ( n ) is any valid hexadecimal, octal or decimal number):</td>
</tr>
<tr>
<td></td>
<td>0xn (CLI assumes hexadecimal format)</td>
</tr>
<tr>
<td></td>
<td>0n (CLI assumes octal format with leading zeros)</td>
</tr>
<tr>
<td></td>
<td>n (CLI assumes decimal format)</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or</td>
</tr>
<tr>
<td></td>
<td>FE80:0:0:0:20F:24FF:FEBF:DBCB, or</td>
</tr>
<tr>
<td></td>
<td>FE80::20F24FF:FEBF:DBCB, or</td>
</tr>
<tr>
<td></td>
<td>FE80:0:0:0:20F:24FF:128:141:49:32</td>
</tr>
<tr>
<td></td>
<td>For additional information, refer to RFC 3513.</td>
</tr>
<tr>
<td>Interface or slot/port</td>
<td>Valid slot and port number separated by a forward slash. For example, 0/1 represents slot number 0 and port number 1.</td>
</tr>
<tr>
<td>Logical Interface</td>
<td>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.</td>
</tr>
<tr>
<td>Character strings</td>
<td>Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.</td>
</tr>
</tbody>
</table>
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

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

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

Table 4: Type of Ports

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

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, 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)
- Routing (Layer 3)
- Multicast
- Quality of Service
- Management (CLI, Web UI 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.

---

**NOTICE**

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

---

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Prompt</th>
<th>Mode Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Switch&gt;</td>
<td>Contains a limited set of commands to view basic system information.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>Switch#</td>
<td>Allows you to issue any EXEC command, enter the VLAN mode, or enter the Global Configuration mode.</td>
</tr>
<tr>
<td>Global Config</td>
<td>Switch (Config)#</td>
<td>Groups general setup commands and permits you to make modifications to the running configuration.</td>
</tr>
<tr>
<td>VLAN Config</td>
<td>Switch (Vlan)#</td>
<td>Groups all the VLAN commands.</td>
</tr>
<tr>
<td>Interface Config</td>
<td>Switch (Interface &lt;slot/port&gt;)#</td>
<td>Manages the operation of an interface and provides access to the router interface configuration commands. Use this mode to set up a physical port for a specific logical connection operation.</td>
</tr>
<tr>
<td></td>
<td>Switch (Interface Loopback &lt;id&gt;)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch (Interface Tunnel &lt;id&gt;)#</td>
<td></td>
</tr>
<tr>
<td>Line Config</td>
<td>Switch (line)#</td>
<td>Contains commands to configure outbound telnet settings and console interface settings.</td>
</tr>
<tr>
<td>Policy Map Config</td>
<td>Switch (Config-policy-map)#</td>
<td>Contains the QoS Policy-Map configuration commands.</td>
</tr>
<tr>
<td>Policy Class Config</td>
<td>Switch (Config-policy-class-map)#</td>
<td>Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.</td>
</tr>
</tbody>
</table>
Table 5: CLI Command Modes (Continued)

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Prompt</th>
<th>Mode Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Map Config</td>
<td>Switch (Config-class-map)#</td>
<td>Contains the QoS class map configuration commands for IPv4.</td>
</tr>
<tr>
<td>MAC Access-list Config</td>
<td>Switch (Config-mac-access-list)#</td>
<td>Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.</td>
</tr>
<tr>
<td>TACACS Config</td>
<td>Switch (Tacacs)#</td>
<td>Contains commands to configure properties for the TACACS servers.</td>
</tr>
<tr>
<td>DHCP Pool Config</td>
<td>Switch (Config dhcp-pool)#</td>
<td>Contains the DHCP server IP address pool configuration commands.</td>
</tr>
</tbody>
</table>

Table 6 explains how to enter or exit each mode.

Table 6: CLI Mode Access and Exit

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>This is the first level of access.</td>
<td>To exit, enter logout.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>From the User EXEC mode, enter enable.</td>
<td>To exit to the User EXEC mode, enter exit or press Ctrl-Z.</td>
</tr>
<tr>
<td>Global Config</td>
<td>From the Privileged EXEC mode, enter configure.</td>
<td>To exit to the Privileged EXEC mode, enter exit or press Ctrl-Z.</td>
</tr>
<tr>
<td>VLAN Config</td>
<td>From the Privileged EXEC mode, enter vlan database.</td>
<td>To exit to the Privileged EXEC mode, enter exit or press Ctrl-Z.</td>
</tr>
<tr>
<td>Interface Config</td>
<td>From the Global Config mode, enter interface &lt;slot/port&gt; or interface loopback &lt;id&gt; or interface tunnel &lt;id&gt;</td>
<td>To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.</td>
</tr>
<tr>
<td>Line Config</td>
<td>From the Global Config mode, enter lineconfig.</td>
<td>To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.</td>
</tr>
<tr>
<td>Policy-Map Config</td>
<td>From the Global Config mode, enter policy-map.</td>
<td>To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.</td>
</tr>
<tr>
<td>Policy-Class-Map Config</td>
<td>From the Policy Map mode enter class.</td>
<td>To exit to the Policy Map mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.</td>
</tr>
<tr>
<td>Class-Map Config</td>
<td>From the Global Config mode, enter class-map, and specify the optional keyword ipv4 to specify the Layer 3 protocol for this class. See 'class-map' on page 195 for more information.</td>
<td>To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.</td>
</tr>
<tr>
<td>MAC Access-list Config</td>
<td>From the Global Config mode, enter mac access-list extended name.</td>
<td>To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.</td>
</tr>
<tr>
<td>TACACS Config</td>
<td>From the Global Config mode, enter tacacs-server host &lt;ip-addr&gt;, where &lt;ip-addr&gt; is the IP address of the TACACS server on your network.</td>
<td>To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.</td>
</tr>
<tr>
<td>DHCP Pool Config</td>
<td>From the Global Config mode, enter ip dhcp pool &lt;pool-name&gt;.</td>
<td>To exit to the Global Config mode, enter exit. To return to the Privileged EXEC mode, enter Ctrl-Z.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Message Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Invalid input detected at '^' marker.</td>
<td>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.</td>
</tr>
<tr>
<td>Command not found / Incomplete command. Use ? to list commands.</td>
<td>Indicates that you did not enter the required keywords or values.</td>
</tr>
<tr>
<td>Ambiguous command</td>
<td>Indicates that you did not enter enough letters to uniquely identify the command.</td>
</tr>
</tbody>
</table>
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

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

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 “Network Interface Commands” on page 501.
2 / Management Commands

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

The Management Commands chapter contains the following sections:
- “Network Interface Commands” on page 22
- “Console Port Access Commands” on page 27
- “Telnet Commands” on page 29
- “Secure Shell Commands” on page 33
- “Management Security Commands” on page 36
- “Hypertext Transfer Protocol Commands” on page 37
- “Access Commands” on page 45
- “User Account Commands” on page 46
- “SNMP Commands” on page 71
- “RADIUS Commands” on page 85
- “TACACS+ Commands” on page 104
- “Configuration Scripting Commands” on page 109
- “Prelogin Banner, System Prompt, and Host Name Commands” on page 111

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 Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see “network mgmt_vlan” on page 325.

2.1.1 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

2.1.2 do (Privileged EXEC commands)

This command executes Privileged EXEC mode commands from any of the configuration modes.

Format

    do Priv Exec Mode Command

Mode

    • Global Config
    • Interface Config
    • VLAN Config
    • Routing Config
**Example:** The following is an example of the `do` command that executes the Privileged EXEC command `script list` in Global Config Mode.

```
(Routing) #configure
(Routing)(config)#do script list
```

<table>
<thead>
<tr>
<th>Configuration Script Name</th>
<th>Size(Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup-config</td>
<td>2165</td>
</tr>
<tr>
<td>running-config</td>
<td>4483</td>
</tr>
<tr>
<td>startup-config</td>
<td>445</td>
</tr>
</tbody>
</table>

3 configuration script(s) found.
2041 Kbytes free.

```
Routing(config)#
```

### 2.1.3 serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port. You can specify the `none` option to clear the IPv4 address and mask and the default gateway (i.e., reset each of these values to 0.0.0.0).

**Format**  
```
serviceport ip {ipaddr netmask [gateway] | none}
```

**Mode**  
Privileged EXEC

### 2.1.4 serviceport protocol

This command specifies the network management port configuration protocol. If you modify this value, the change is effective immediately. If you use the `bootp` parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the `dhcp` parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the `none` parameter, you must configure the network information for the switch manually.

**Format**  
```
serviceport protocol {none | bootp | dhcp}
```

**Mode**  
Privileged EXEC

### 2.1.5 serviceport protocol dhcp

This command enables the DHCPv4 client on a Service port. If the `client-id` optional parameter is given, the DHCP client messages are sent with the client identifier option.

**Default**  
```
none
```

**Format**  
```
serviceport protocol dhcp [client-id]
```

**Mode**  
Privileged EXEC

There is no support for the no form of the command `serviceport protocol dhcp client-id`. To remove the `client-id` option from the DHCP client messages, issue the command `serviceport protocol dhcp` without the `client-id` option. The command `serviceport protocol none` can be used to disable the DHCP client and client-id option on the interface.

**Example:** The following shows an example of the command.

```
(Routing) # serviceport protocol dhcp client-id
```
2.1.6   **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. When you specify the `none` option, the IP address and subnet mask are set to the factory defaults.

**Format**

```
network parms {ipaddr netmask [gateway]} none
```

**Mode**

Privileged EXEC.

2.1.7   **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

2.1.8   **network protocol dhcp**

This command enables the DHCPv4 client on a Network port. If the `client-id` optional parameter is given, the DHCP client messages are sent with the client identifier option.

**Default**

`none`

**Format**

```
network protocol dhcp [client-id]
```

**Mode**

Global Config

There is no support for the no form of the command network protocol dhcp client-id. To remove the `client-id` option from the DHCP client messages, issue the command network protocol dhcp without the `client-id` option. The command network protocol none can be used to disable the DHCP client and client-id option on the interface.

**Example:** The following shows an example of the command.

```
(Routing) # network protocol dhcp client-id
```

2.1.9   **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
2.1.10 **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

2.1.10.1 **no network mac-type**

This command resets the value of MAC address to its default.

- **Format**: `no network mac-type`
- **Mode**: Privileged EXEC

2.1.11 **network javamode**

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the Web interface. When access is enabled, the Java applet can be viewed from the Web interface. When access is disabled, the user cannot view the Java applet.

- **Default**: enabled
- **Format**: `network javamode`
- **Mode**: Privileged EXEC

2.1.11.1 **no network javamode**

This command disallows access to the Java applet in the header frame of the Web interface. When access is disabled, the user cannot view the Java applet.

- **Format**: `no network javamode`
- **Mode**: Privileged EXEC

2.1.12 **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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Status</td>
<td>The network interface status; it is always considered to be “up”.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the interface. The factory default value is 0.0.0.0.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The IP subnet mask for this interface. The factory default value is 0.0.0.0.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The default gateway for this IP interface. The factory default value is 0.0.0.0.</td>
</tr>
<tr>
<td>IPv6 Administrative Mode</td>
<td>Whether enabled or disabled.</td>
</tr>
<tr>
<td>IPv6 Address/Length</td>
<td>The IPv6 address and length.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the network port.

```
(admin) #show network

Interface Status............................ Up
IP Address-------------------------------- 10.250.3.1
Subnet Mask------------------------------- 255.255.255.0
Default Gateway------------------------- 10.250.3.3
IPv6 Administrative Mode.................. Enabled
IPv6 Prefix is ............................ Fe80::210:18ff:fe82:64c/64
IPv6 Prefix is ............................ 2003::1/128
IPv6 Default Router is ...................... fe80::204:76ff:fe73:423a
Burned In MAC Address...................... 00:10:18:82:06:4C
Locally Administered MAC address........... 00:00:00:00:00:00
MAC Address Type............................ Burned In
Configured IPv4 Protocol .................... None
Configured IPv6 Protocol .................... DHCP
DHCPv6 Client DUID.......................... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode....................... Disabled
Management VLAN ID.......................... 1
DHCP Client Identifier..................... 0fastpath-0010.1882.160B-v11
```

2.1.13 show serviceport

This command displays service port configuration information.

Format show serviceport

Mode
- Privileged EXEC
- User EXEC
Example: The following shows example CLI display output for the service port.

```
(admin) #show serviceport
```

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Status</td>
<td>The network interface status. It is always considered to be up.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the interface. The factory default value is 0.0.0.0.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The IP subnet mask for this interface. The factory default value is 0.0.0.0.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The default gateway for this IP interface. The factory default value is 0.0.0.0.</td>
</tr>
<tr>
<td>IPv6 Administrative Mode</td>
<td>Whether enabled or disabled. Default value is enabled.</td>
</tr>
<tr>
<td>IPv6 Address/Length</td>
<td>The IPv6 address and length. Default is Link Local format.</td>
</tr>
<tr>
<td>IPv6 Default Router</td>
<td>The IPv6 default router address on the service port. The factory default value is an unspecified address.</td>
</tr>
<tr>
<td>Configured IPv4 Protocol</td>
<td>The IPv4 network protocol being used. The options are bootp</td>
</tr>
<tr>
<td>Configured IPv6 Protocol</td>
<td>The IPv6 network protocol being used. The options are dhcp</td>
</tr>
<tr>
<td>DHCPv6 Client DUID</td>
<td>The DHCPv6 client’s unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.</td>
</tr>
<tr>
<td>IPv6 Autoconfig Mode</td>
<td>Whether IPv6 Stateless address autoconfiguration is enabled or disabled.</td>
</tr>
<tr>
<td>Burned in MAC Address</td>
<td>The burned in MAC address used for in-band connectivity.</td>
</tr>
<tr>
<td>DHCP Client Identifier</td>
<td>The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the service port.</td>
</tr>
</tbody>
</table>

2.2 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.

2.2.1 configure

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.

<table>
<thead>
<tr>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>
2.2.2 **line**
This command gives you access to the Line Console mode, which allows you to configure various Telnet settings and the console port, as well as to configure console login/enable authentication.
Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

**Format**
```
line {console | telnet | ssh}
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>console</td>
<td>Console terminal line.</td>
</tr>
<tr>
<td>telnet</td>
<td>Virtual terminal for remote console access (Telnet).</td>
</tr>
<tr>
<td>ssh</td>
<td>Virtual terminal for secured remote console access (SSH).</td>
</tr>
</tbody>
</table>

*Example:* The following shows an example of the CLI command.

```text
(FASTPATH Routing)(config)#line telnet
(FASTPATH Routing)(config-telnet)#
```

2.2.3 **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

2.2.3.1 **no serial baudrate**
This command sets the communication rate of the terminal interface.

**Format**
```
no serial baudrate
```

**Mode**
Line Config

2.2.4 **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
2.2.4.1  no serial timeout
This command sets the maximum connect time (in minutes) without console activity.

**Format**  
no serial timeout

**Mode**  
Line Config

2.2.5  show serial
This command displays serial communication settings for the switch.

**Format**  
show serial

**Modes**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Port Login Timeout (minutes)</td>
<td>The time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. A value of 0 disables the timeout.</td>
</tr>
<tr>
<td>Baud Rate (bps)</td>
<td>The default baud rate at which the serial port will try to connect.</td>
</tr>
<tr>
<td>Character Size (bits)</td>
<td>The number of bits in a character. The number of bits is always 8.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>The number of Stop bits per character. The number of Stop bits is always 1.</td>
</tr>
<tr>
<td>Parity</td>
<td>The parity method used on the Serial Port. The Parity Method is always None.</td>
</tr>
</tbody>
</table>

2.3  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.

2.3.1  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
2.3.1.1  **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

2.3.2  **ip telnet port**
This command configures the TCP port number on which the Telnet server listens for requests.

**Default**  
23

**Format**  
ip telnet port 1-65535

**Mode**  
Privileged EXEC

2.3.2.1  **no ip telnet port**
This command restores the Telnet server listen port to its factory default value.

**Format**  
o ip telnet port

**Mode**  
Privileged EXEC

2.3.3  **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 localecho option enables local echo.

**Format**  
telnet ip-address|hostname port [debug] [line] [localecho]

**Modes**  
- Privileged EXEC
- User EXEC

2.3.4  **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.

---

**NOTICE**
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
2.3.4.1 no transport input telnet
Use this command to prevent new Telnet sessions from being established.

 Format  no transport input telnet
 Mode    Line Config

2.3.5 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

2.3.5.1 no transport output telnet
Use this command to prevent new outbound Telnet connection from being established.

 Format  no transport output telnet
 Mode    Line Config

2.3.6 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

2.3.6.1 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

2.3.7 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
2.3.7.1  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

2.3.8  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

2.3.8.1  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

2.3.9  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.

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

2.3.9.1  no telnetcon timeout
This command sets the Telnet connection session timeout value to the default.

Changing the timeout value for active sessions does not become effective until the session is accessed again. Also, any keystroke activates the new timeout duration.

Format           no telnetcon timeout
Mode             Privileged EXEC
2.3.10 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Telnet Login Timeout</td>
<td>The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.</td>
</tr>
<tr>
<td>Maximum Number of Outbound Telnet Sessions</td>
<td>The number of simultaneous outbound Telnet connections allowed.</td>
</tr>
<tr>
<td>Allow New Outbound Telnet Sessions</td>
<td>Indicates whether outbound Telnet sessions will be allowed.</td>
</tr>
</tbody>
</table>

2.3.11 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Connection Login Timeout (minutes)</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Number of Remote Connection Sessions</td>
<td>This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.</td>
</tr>
<tr>
<td>Allow New Telnet Sessions</td>
<td>New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.</td>
</tr>
<tr>
<td>Telnet Server Admin Mode</td>
<td>If Telnet Admin mode is enabled or disabled.</td>
</tr>
<tr>
<td>Telnet Server Port</td>
<td>The configured TCP port number on which the Telnet server listens for requests. (The default is 23.)</td>
</tr>
</tbody>
</table>

2.4 Secure Shell Commands

This section describes the commands you use to configure Secure Shell (SSH) access to the switch. Use SSH to access the switch from a remote management host.

The system allows a maximum of 5 SSH sessions.
2.4.1 ip ssh
Use this command to enable SSH access to the system. (This command is the short form of the `ip ssh server enable` command)

Default: disabled
Format: `ip ssh`
Mode: Privileged EXEC

2.4.2 ip ssh port
Use this command to configure the TCP port number on which the SSH server listens for requests. Valid port numbers are from 1–65535.

Default: 22
Format: `ip ssh port 1-65535`
Mode: Privileged EXEC

2.4.2.1 no ip ssh port
Use this command to restore the SSH server listen port to its factory default value.

Format: `no ip ssh port`
Mode: Privileged EXEC

2.4.3 ip ssh protocol
This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default: 2
Format: `ip ssh protocol [1] [2]`
Mode: Privileged EXEC

2.4.4 ip ssh server enable
This command enables the IP secure shell server. No new SSH connections are allowed, but the existing SSH connections continue to work until timed-out or logged-out.

Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

Default: enabled
Format: `ip ssh server enable`
Mode: Privileged EXEC
2.4.4.1 **no ip ssh server enable**
This command disables the IP secure shell server.

**Format**
```
no ip ssh server enable
```

**Mode**
Privileged EXEC

2.4.5 **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

2.4.5.1 **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

2.4.6 **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 key-stroke activates the new timeout duration.

**Default**
5

**Format**
```
sshcon timeout 1-160
```

**Mode**
Privileged EXEC
2.4.6.1 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 key-stroke activates the new timeout duration.

Format  
no sshcon timeout

Mode  
Privileged EXEC

2.4.7 show ip ssh

This command displays the ssh settings.

Format  
show ip ssh

Mode  
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Mode</td>
<td>This field indicates whether the administrative mode of SSH is enabled or disabled.</td>
</tr>
<tr>
<td>Protocol Level</td>
<td>The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.</td>
</tr>
<tr>
<td>SSH Sessions Currently Active</td>
<td>The number of SSH sessions currently active.</td>
</tr>
<tr>
<td>Max SSH Sessions Allowed</td>
<td>The maximum number of SSH sessions allowed.</td>
</tr>
<tr>
<td>SSH Timeout</td>
<td>The SSH timeout value in minutes.</td>
</tr>
<tr>
<td>Keys Present</td>
<td>Indicates whether the SSH RSA and DSA key files are present on the device.</td>
</tr>
<tr>
<td>Key Generation in Progress</td>
<td>Indicates whether RSA or DSA key files generation is currently in progress.</td>
</tr>
</tbody>
</table>

2.5 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.

2.5.1 crypto certificate generate

Use this command to generate a self-signed certificate for HTTPS. The generated 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
2.5.1.1 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

2.5.2 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

2.5.2.1 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

2.5.3 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

2.5.3.1 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

2.6 Hypertext Transfer Protocol Commands
This section describes the commands you use to configure Hypertext Transfer Protocol (HTTP) and secure HTTP access to the switch. Access to the switch by using a Web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the Web.

2.6.1 ip http accounting exec, ip https accounting exec
This command applies user exec (start-stop/stop-only) accounting list to the line methods HTTP and HTTPS. Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

---

**NOTICE**
The user exec accounting list should be created using the command “aaa accounting” on page 66.
2.6.1.1 no ip http/https accounting exec

This command deletes the authorization method list.

**Format**

```
no ip {http|https} accounting exec {default|listname}
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http/https</td>
<td>The line method for which the list needs to be applied.</td>
</tr>
<tr>
<td>default</td>
<td>The default list of methods for authorization services.</td>
</tr>
<tr>
<td>listname</td>
<td>An alphanumeric character string used to name the list of accounting methods.</td>
</tr>
</tbody>
</table>

2.6.2 ip http authentication

Use this command to specify authentication methods for http server users. The default configuration is the local user database is checked. This action has the same effect as the command `ip http authentication local`. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

**Default**

```
local
```

**Format**

```
ip http authentication method1 [method2...]
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

**Example:** The following example configures the http authentication.

```
(switch)(config)# ip http authentication radius local
```

2.6.2.1 no ip http authentication

Use this command to return to the default.

**Format**

```
no ip http authentication
```

**Mode**

Global Config
2.6.3 ip https authentication

Use this command to specify authentication methods for https server users. The default configuration is the local user database is checked. This action has the same effect as the command ip https authentication local. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. For example, if none is specified as an authentication method after radius, no authentication is used if the RADIUS server is down.

Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

Default local

Format ip https authentication method1 [method2...]

Mode Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td>radius</td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS+ servers for authentication.</td>
</tr>
</tbody>
</table>

**Example:** The following example configures https authentication.

```
(switch)(config)# ip https authentication radius local
```

2.6.3.1 no ip https authentication

Use this command to return to the default.

Format no ip https authentication

Mode Global Config

2.6.4 ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Default enabled

Format ip http server

Mode Privileged EXEC
2.6.4.1  **no ip http server**  
This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

**Format**  
no ip http server

**Mode**  
Privileged EXEC

2.6.5  **ip http secure-server**  
This command is used to enable the secure socket layer for secure HTTP.

**Default**  
disabled

**Format**  
ip http secure-server

**Mode**  
Privileged EXEC

2.6.5.1  **no ip http secure-server**  
This command is used to disable the secure socket layer for secure HTTP.

**Format**  
no ip http secure-server

**Mode**  
Privileged EXEC

2.6.6  **ip http java**  
This command enables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

**Default**  
Enabled

**Format**  
ip http java

**Mode**  
Privileged EXEC

2.6.6.1  **no ip http java**  
This command disables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

**Format**  
no ip http java

**Mode**  
Privileged EXEC

2.6.7  **ip http port**  
This command configures the TCP port number on which the HTTP server listens for requests.

**Default**  
80

**Format**  
ip http port 1-65535

**Mode**  
Privileged EXEC
2.6.7.1  no ip http port
This command restores the HTTP server listen port to its factory default value.

Format   no ip http port
Mode     Privileged EXEC

2.6.8  ip http rest-api port
This command configures the HTTP TCP port number on which the OpEN restful API server listens for restful requests.

Default  8080
Format    ip http rest-api port 1025-65535
Mode      Privileged EXEC

2.6.8.1  no ip http rest-api port
This command restores the OpEN restful API HTTP server listen port to its factory default value.

Format   no ip http rest-api port
Mode     Privileged EXEC

2.6.9  ip http rest-api secure-port
This command configures the HTTPS TCP port number on which the OpEN restful API server listens for secure restful requests.

Default  8443
Format    ip http rest-api secure-port 1025-65535
Mode      Privileged EXEC

2.6.10  no ip http rest-api secure-port
This command restores the OpEN restful API HTTP server listen port to its factory default value.

Format   no ip http rest-api secure-port
Mode     Privileged EXEC

2.6.9  ip http session hard-timeout
This command configures the hard timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite hard-timeout. When this timeout expires, the user will be forced to reauthenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default  24
Format    ip http session hard-timeout 1-168
Mode      Privileged EXEC
2.6.10.1  no ip http session hard-timeout
This command restores the hard timeout for un-secure HTTP sessions to the default value.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip http session hard-timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

2.6.11  ip http session maxsessions
This command limits the number of allowable un-secure HTTP sessions. Zero is the configurable minimum.

<table>
<thead>
<tr>
<th>Default</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip http session maxsessions 0-16</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

2.6.11.1  no ip http session maxsessions
This command restores the number of allowable un-secure HTTP sessions to the default value.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip http session maxsessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

2.6.12  ip http session soft-timeout
This command configures the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to reauthenticate. This timer begins on initiation of the Web session and is restarted with each access to the switch.

<table>
<thead>
<tr>
<th>Default</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip http session soft-timeout 1-60</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

2.6.12.1  no ip http session soft-timeout
This command resets the soft timeout for un-secure HTTP sessions to the default value.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip http session soft-timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

2.6.13  ip http secure-session hard-timeout
This command configures the hard timeout for secure HTTP sessions in hours. When this timeout expires, the user is forced to reauthenticate. This timer begins on initiation of the Web session and is unaffected by the activity level of the connection. The secure-session hard-timeout can not be set to zero (infinite).

<table>
<thead>
<tr>
<th>Default</th>
<th>24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip http secure-session hard-timeout 1-168</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>
2.6.13.1  no ip http secure-session hard-timeout
This command resets the hard timeout for secure HTTP sessions to the default value.

**Format**  
no ip http secure-session hard-timeout

**Mode**  
Privileged EXEC

2.6.14  ip http secure-session maxsessions
This command limits the number of secure HTTP sessions. Zero is the configurable minimum.

**Default**  
16

**Format**  
ip http secure-session maxsessions \(0-16\)

**Mode**  
Privileged EXEC

2.6.14.1  no ip http secure-session maxsessions
This command restores the number of allowable secure HTTP sessions to the default value.

**Format**  
no ip http secure-session maxsessions

**Mode**  
Privileged EXEC

2.6.15  ip http secure-session soft-timeout
This command configures the soft timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, you are forced to reauthenticate. This timer begins on initiation of the Web session and is restarted with each access to the switch. The secure-session soft-timeout can not be set to zero (infinite).

**Default**  
5

**Format**  
ip http secure-session soft-timeout \(1-60\)

**Mode**  
Privileged EXEC

2.6.15.1  no ip http secure-session soft-timeout
This command restores the soft timeout for secure HTTP sessions to the default value.

**Format**  
no ip http secure-session soft-timeout

**Mode**  
Privileged EXEC

2.6.16  ip http secure-port
This command is used to set the SSL port where port can be 1025-65535 and the default is port 443.

**Default**  
443

**Format**  
ip http secure-port \(portid\)

**Mode**  
Privileged EXEC
2.6.16.1 no ip http secure-port
This command is used to reset the SSL port to the default value.

**Format**

```
no ip http secure-port
```

**Mode**

Privileged EXEC

2.6.17 ip http secure-protocol
This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

**Default**

SSL3 and TLS1

**Format**

```
ip http secure-protocol [SSL3] [TLS1]
```

**Mode**

Privileged EXEC

2.6.18 show ip http
This command displays the http settings for the switch.

**Format**

```
show ip http
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Mode (Unsecure)</td>
<td>The unsecure HTTP server administrative mode.</td>
</tr>
<tr>
<td>Java Mode</td>
<td>The Java applet administrative mode which applies to both secure and un-secure web connections.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>The configured TCP port on which the HTTP server listens for requests. (The default is 80.)</td>
</tr>
<tr>
<td>RESTful API HTTP Port</td>
<td>The HTTPS TCP port number on which the OpEN RESTful API server listens for RESTful requests.</td>
</tr>
<tr>
<td>RESTful API HTTPS Port</td>
<td>The HTTPS TCP port number on which the OpEN RESTful API server listens for secure RESTful requests.</td>
</tr>
<tr>
<td>Maximum Allowable HTTP Sessions</td>
<td>The number of allowable un-secure http sessions.</td>
</tr>
<tr>
<td>HTTP Session Hard Timeout</td>
<td>The hard timeout for un-secure http sessions in hours.</td>
</tr>
<tr>
<td>HTTP Session Soft Timeout</td>
<td>The soft timeout for un-secure http sessions in minutes.</td>
</tr>
<tr>
<td>HTTP Mode (Secure)</td>
<td>The secure HTTP server administrative mode.</td>
</tr>
<tr>
<td>Secure Port</td>
<td>The secure HTTP server port number.</td>
</tr>
<tr>
<td>Secure Protocol Level(s)</td>
<td>The protocol level may have the values of SSL3, TSL1, or both SSL3 and SSL1.</td>
</tr>
<tr>
<td>Maximum Allowable HTTPS Sessions</td>
<td>The number of allowable secure http sessions.</td>
</tr>
<tr>
<td>HTTPS Session Hard Timeout</td>
<td>The hard timeout for secure http sessions in hours.</td>
</tr>
<tr>
<td>HTTPS Session Soft Timeout</td>
<td>The soft timeout for secure http sessions in minutes.</td>
</tr>
<tr>
<td>Certificate Present</td>
<td>Indicates whether the secure-server certificate files are present on the device.</td>
</tr>
<tr>
<td>Certificate Generation in Progress</td>
<td>Indicates whether certificate generation is currently in progress.</td>
</tr>
</tbody>
</table>
2.7 Access Commands

Use the commands in this section to close remote connections or to view information about connections to the system.

2.7.1 disconnect

Use the disconnect command to close HTTP, HTTPS, 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.

Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

Format: 
```
disconnect {session_id | all}
```
Mode: Privileged EXEC

2.7.2 linuxsh

Use the linuxsh command to access the Linux shell. Use the exit command to exit the Linux shell and return to the CLI. The shell session will timeout after five minutes of inactivity. The inactivity timeout value can be changed using the command "session-timeout" on page 31 in Line Console mode.

Default: ip-port:2324
Format: 
```
linuxsh [ip-port]
```
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-port</td>
<td>The IP port number on which the telnet daemon listens for connections. ip-port is an integer from 1 to 65535. The default value is 2324.</td>
</tr>
</tbody>
</table>

2.7.3 show loginsession

This command displays current Telnet, SSH and serial port connections to the switch. This command displays truncated user names. Use the show loginsession long command to display the complete usernames.

Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

Format: show loginsession
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Login Session ID.</td>
</tr>
<tr>
<td>User Name</td>
<td>The name the user entered to log on to the system.</td>
</tr>
<tr>
<td>Connection From</td>
<td>IP address of the remote client machine or ELA-232 for the serial port connection.</td>
</tr>
<tr>
<td>Idle Time</td>
<td>Time this session has been idle.</td>
</tr>
<tr>
<td>Session Time</td>
<td>Total time this session has been connected.</td>
</tr>
<tr>
<td>Session Type</td>
<td>Shows the type of session, which can be HTTP, HTTPS, telnet, serial, or SSH.</td>
</tr>
</tbody>
</table>
2.7.4 show loginsession long

This command displays the complete user names of the users currently logged in to the switch.

**Format**

    show loginsession long

**Mode**

    Privileged EXEC

**Example:** The following shows an example of the command.

    (switch) #show loginsession long
    User Name
    ------------
    admin
test111test111test111test111test111test111test111test111

2.8 User Account Commands

This section describes the commands you use to add, manage, and delete system users. FASTPATH software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

You cannot delete the admin user. There is only one user allowed with level-15 privileges. You can configure up to five level-1 users on the system.

**Notice**

Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

2.8.1 aaa authentication login

Use this command to set authentication at login. The default and optional list names created with the command are used with the `aaa authentication login` command. Create a list by entering the `aaa authentication login list-name method` command, where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

**Default**

- `defaultList`. Used by the console and only contains the method `none`.
- `networkList`. Used by telnet and SSH and only contains the method `local`.

**Format**

    aaa authentication login {default | list-name} method1 [method2...]

**Mode**

    Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.</td>
</tr>
<tr>
<td>list-name</td>
<td>Character string of up to 15 characters used to name the list of authentication methods activated when a user logs in.</td>
</tr>
</tbody>
</table>
Example: The following shows an example of the command.

(switch)(config)# aaa authentication login default radius local enable none

2.8.1.1 no aaa authentication login

This command returns to the default.

Format: aaa authentication login {default | list-name}

Mode: Global Config

2.8.2 aaa authentication enable

Use this command to set authentication for accessing higher privilege levels. The default enable list is enableList. It is used by console, and contains the method as enable followed by none.

A separate default enable list, enableNetList, is used for Telnet and SSH users instead of enableList. This list is applied by default for Telnet and SSH, and contains enable followed by deny methods. In FASTPATH, by default, the enable password is not configured. That means that, by default, Telnet and SSH users will not get access to Privileged EXEC mode. On the other hand, with default conditions, a console user always enter the Privileged EXEC mode without entering the enable password.

The default and optional list names created with the aaa authentication enable command are used with the enable authentication command. Create a list by entering the aaa authentication enable list-name method command where list-name is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries in the given sequence.

The user manager returns ERROR (not PASS or FAIL) for enable and line methods if no password is configured, and moves to the next configured method in the authentication list. The method none reflects that there is no authentication needed.

The user will only be prompted for an enable password if one is required. The following authentication methods do not require passwords:

1. none
2. deny
3. enable (if no enable password is configured)
4. line (if no line password is configured)

Example: See the examples below.

   a. aaa authentication enable default enable none
   b. aaa authentication enable default line none
   c. aaa authentication enable default enable radius none
   d. aaa authentication enable default line tacacs none

Examples a and b do not prompt for a password, however because examples c and d contain the radius and tacacs methods, the password prompt is displayed.
If the login methods include only enable, and there is no enable password configured, then FASTPATH does not prompt for a username. In such cases, FASTPATH only prompts for a password. FASTPATH supports configuring methods after the local method in authentication and authorization lists. If the user is not present in the local database, then the next configured method is tried.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

Use the command `show authorization methods` on page 51 to display information about the authentication methods.

**Example:** The following example sets authentication when accessing higher privilege levels.

```
(switch)(config)# aaa authentication enable {default | list-name} method1 [method2...]
```

### 2.8.2.1 no aaa authentication enable

Use this command to return to the default configuration.

**Format**

```
no aaa authentication enable {default | list-name}
```

**Mode**

Global Config

### 2.8.3 aaa authorization

Use this command to configure command and exec authorization method lists. This list is identified by `default` or a user-specified `list-name`. If `tacacs` is specified as the authorization method, authorization commands are notified to a TACACS-server. If `none` is specified as the authorization method, command authorization is not applicable. A maximum of five authorization method lists can be created for the `commands` type.

**Notice:** Local method is not supported for command authorization. Command authorization with RADIUS will work if, and only if, the applied authentication method is also `radius`.

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.</td>
</tr>
<tr>
<td>list-name</td>
<td>Character string used to name the list of authentication methods activated, when using access higher privilege levels. Range: 1-15 characters.</td>
</tr>
</tbody>
</table>
| method1 [method2...] | Specify at least one from the following:  
  - `deny`. Used to deny access.  
  - `enable`. Uses the enable password for authentication.  
  - `line`. Uses the line password for authentication.  
  - `none`. Uses no authentication.  
  - `radius`. Uses the list of all RADIUS servers for authentication.  
  - `tacacs`. Uses the list of all TACACS+ servers for authentication. |
2.8.3.1 Per-Command Authorization

When authorization is configured for a line mode, the user manager sends information about an entered command to the AAA server. The AAA server validates the received command, and responds with either a PASS or FAIL response. If approved, the command is executed. Otherwise, the command is denied and an error message is shown to the user. The various utility commands like tftp, ping, and outbound telnet should also pass command authorization. Applying the script is treated as a single command apply script, which also goes through authorization. Startup-config commands applied on device boot-up are not an object of the authorization process.

The per-command authorization usage scenario is this:

1. Configure Authorization Method List
   aaa authorization commands listname tacacs radius none
2. Apply AML to an Access Line Mode (console, telnet, SSH)
   authorization commands listname
3. Commands entered by the user will go through command authorization via TACACS+ or RADIUS server and will be accepted or denied.

2.8.3.2 Exec Authorization

When exec authorization is configured for a line mode, the user may not be required to use the enable command to enter Privileged EXEC mode. If the authorization response indicates that the user has sufficient privilege levels for Privileged EXEC mode, then the user bypasses User EXEC mode entirely.

The exec authorization usage scenario is this:

1. Configure Authorization Method List
   aaa authorization exec listname method1 [method2....]
2. Apply AML to an Access Line Mode (console, telnet, SSH)
   authorization exec listname
3. When the user logs in, in addition to authentication, authorization will be performed to determine if the user is allowed direct access to Privileged EXEC mode.

**Format**

```
aaa authorization {commands|exec} {default|list-name} method1[method2]
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commands</td>
<td>Provides authorization for all user-executed commands.</td>
</tr>
<tr>
<td>exec</td>
<td>Provides exec authorization.</td>
</tr>
<tr>
<td>default</td>
<td>The default list of methods for authorization services.</td>
</tr>
<tr>
<td>list-name</td>
<td>Alphanumeric character string used to name the list of authorization methods.</td>
</tr>
<tr>
<td>method</td>
<td>TACACS+/RADIUS/Local and none are supported.</td>
</tr>
</tbody>
</table>

**Example:** The following shows an example of the command.

```
(FASTPATH Routing) #
(FASTPATH Routing) #configure
(FASTPATH Routing) (Config)#aaa authorization exec default tacacs+ none
(FASTPATH Routing) (Config)#aaa authorization commands default tacacs+ none
```
2.8.3.3  no aaa authorization
This command deletes the authorization method list.

**Format**  
no aaa authorization {commands|exec} {default|list-name}

**Mode**  
Global Config

2.8.4  authorization commands
This command applies a command authorization method list to an access method (console, telnet, ssh). For usage scenarios on per command authorization, see the command "aaa authorization" on page 48.

**Format**  
authorization commands [default|list-name]

**Mode**  
Line console, Line telnet, Line SSH

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commands</td>
<td>This causes command authorization for each command execution attempt.</td>
</tr>
</tbody>
</table>

2.8.4.1  no authorization commands
This command removes command authorization from a line config mode.

**Format**  
no authorization {commands|exec}

**Mode**  
Line console, Line telnet, Line SSH

**Example:** The following shows an example of the command.

(Switching) (Config)#line console
(Switching) (Config-line)#authorization commands list2

(Switching) (Config-line)#
(Switching) (Config-line)#exit

(FASTPATH Switching) (Config)#

2.8.5  authorization exec
This command applies a command authorization method list to an access method so that the user may not be required to use the enable command to enter Privileged EXEC mode. For usage scenarios on exec authorization, see the command "aaa authorization" on page 48.

**Format**  
authorization exec list-name

**Mode**  
Line console, Line telnet, Line SSH

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>The command authorization method list.</td>
</tr>
</tbody>
</table>
2.8.5.1  no authorization exec
This command removes command authorization from a line config mode.

Format  no authorization exec
Mode    Line console, Line telnet, Line SSH

2.8.6    authorization exec default
This command applies a default command authorization method list to an access method so that the user may not be required to use the enable command to enter Privileged EXEC mode. For usage scenarios on exec authorization, see the command “aaa authorization” on page 48.

Format  authorization exec default
Mode    Line console, Line telnet, Line SSH

2.8.6.1  no authorization exec default
This command removes command authorization from a line config mode.

Format  no authorization exec default
Mode    Line console, Line telnet, Line SSH

2.8.7    show authorization methods
This command displays the configured authorization method lists.

Format  show authorization methods
Mode    Privileged EXEC

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

(Switching) #show authorization methods

<table>
<thead>
<tr>
<th>Command Authorization List</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>dfltCmdAuthList</td>
<td>tacacs</td>
</tr>
<tr>
<td>list2</td>
<td>none</td>
</tr>
<tr>
<td>list4</td>
<td>tacacs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Line</th>
<th>Command Method List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>dfltCmdAuthList</td>
</tr>
<tr>
<td>Telnet</td>
<td>dfltCmdAuthList</td>
</tr>
<tr>
<td>SSH</td>
<td>dfltCmdAuthList</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exec Authorization List</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>dfltExecAuthList</td>
<td>tacacs</td>
</tr>
<tr>
<td>list2</td>
<td>none</td>
</tr>
<tr>
<td>list4</td>
<td>tacacs</td>
</tr>
</tbody>
</table>

Formatted no authorization exec
Mode Line console, Line telnet, Line SSH

Formatted no authorization exec default
Mode Line console, Line telnet, Line SSH

Formatted show authorization methods
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.
Line Exec Method List

<table>
<thead>
<tr>
<th>Method</th>
<th>List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>dfltExecAuthList</td>
</tr>
<tr>
<td>Telnet</td>
<td>dfltExecAuthList</td>
</tr>
<tr>
<td>SSH</td>
<td>dfltExecAuthList</td>
</tr>
</tbody>
</table>

2.8.8 enable authentication

Use this command to specify the authentication method list when accessing a higher privilege level from a remote telnet or console.

**Format**

```
enable authentication {default | list-name}
```

**Mode**

Line Config

**Example:** The following example specifies the default authentication method when accessing a higher privilege level console.

```
(switch)(config)# line console
(switch)(config-line)# enable authentication default
```

2.8.8.1 no enable authentication

Use this command to return to the default specified by the `enable authentication` command.

**Format**

```
no enable authentication
```

**Mode**

Line Config

2.8.9 username (Global Config)

Use the `username` command in Global Config mode to add a new user to the local user database. The default privilege level is 1. Using the `encrypted` keyword allows the administrator to transfer local user passwords between devices without having to know the passwords. When the `password` parameter is used along with `encrypted` parameter, the password must be exactly 128 hexadecimal characters in length. If the password strength feature is enabled, this command checks for password strength and returns an appropriate error if it fails to meet the password strength criteria. Giving the optional parameter `override-complexity-check` disables the validation of the password strength.

**Format**

```
username name {password password [encrypted [override-complexity-check] | level level [encrypted [override-complexity-check]] | override-complexity-check]} | {level level [override-complexity-check] password}
```

**Mode**

Global Config

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the user. Range: 1-64 characters.</td>
</tr>
<tr>
<td>password</td>
<td>The authentication password for the user. Range 8-64 characters. This value can be zero if the <code>no passwords min-length</code> command has been executed. The special characters allowed in the password include ! # $ % &amp; ' ( ) * + , - . / ; &lt; = &gt; @ <code>[ </code> ^ _ `{</td>
</tr>
<tr>
<td>level</td>
<td>The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user’s access. Range 0-15. Enter access level 1 for <code>non-privileged</code> (switch&gt; prompt) or 15 for highest privilege (switch# prompt) Access. If not specified where it is optional, the privilege level is 1.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypted password entered, copied from another switch configuration.</td>
</tr>
<tr>
<td>override-complexity-check</td>
<td>Disables the validation of the password strength.</td>
</tr>
</tbody>
</table>
**Example:** The following example configures user `bob` with password `xxxxyyyymmmm` and user level 15.

```
(switch)(config)# username bob password xxxyyymmmm level 15
```

**Example:** The following example configures user `test` with password `testPassword` and assigns a user level of 1. The password strength will not be validated.

```
(switch)(config)# username test password testPassword level 1 override-complexity-check
```

**Example:** A third example.

```
(Switching) (Config)# username test password testtest
```

**Example:** A fourth example.

```
(Switching) (Config)# username test password e8d6367774143114ff9e39a853a15e8f35ad059e2e1b49816c243d7e80152b052eafbf23b528d348cda1b1b7ab91be84
227e5e970dbfc62d16dcd13c0b864 level 1 encrypted override-complexity-check
```

```
(Switching) (Config)# username test level 15 password
```

Enter new password:********

Confirm new password:********

**Example:** A fifth example.

```
(Switching) (Config)# username test level 15 override-complexity-check password
```

Enter new password:********

Confirm new password:********

2.8.9.1 no username

Use this command to remove a user name.

```
Format           no username name
Mode            Global Config
```

2.8.10 username nopassword

Use this command to remove an existing user’s password (NULL password).

```
Format           username name nopassword [level level]
Mode            Global Config
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the user. Range: 1-32 characters.</td>
</tr>
<tr>
<td>password</td>
<td>The authentication password for the user. Range 8-64 characters.</td>
</tr>
<tr>
<td>level</td>
<td>The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user’s access. Range 0-15.</td>
</tr>
</tbody>
</table>
2.8.11 username unlock

Use this command to allows a locked user account to be unlocked. Only a user with Level 1 access can reactivate a locked user account.

Format username name unlock
Mode Global Config

2.8.12 username snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are readonly or readwrite. The username is the login user name for which the specified access mode applies. The default is readwrite for the "admin" user and readonly for all other users. You must enter the username in the same case you used when you added the user. To see the case of the username, enter the show users command.

Defaults
- admin - readwrite
- other - readonly

Format username snmpv3 accessmode username {readonly | readwrite}
Mode Global Config

2.8.12.1 no username snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified user as readwrite for the "admin" user and readonly for all other users. The username value is the user name for which the specified access mode will apply.

Format no username snmpv3 accessmode username
Mode Global Config

2.8.13 username snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are none, md5 or sha. If you specify md5 or sha, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The username is the user name associated with the authentication protocol. You must enter the username in the same case you used when you added the user. To see the case of the username, enter the show users command.

Default no authentication

Format username snmpv3 authentication username {none | md5 | sha}
Mode Global Config
2.8.13.1 no username snmpv3 authentication
This command sets the authentication protocol to be used for the specified user to none. The username is the user name for which the specified authentication protocol is used.

Format
no username snmpv3 authentication username
Mode
Global Config

2.8.14 username snmpv3 encryption
This command specifies the encryption protocol used for the specified user. The valid encryption protocols are des or none.

If you select des, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the des protocol but do not provide a key, the user is prompted for the key. When you use the des protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select none, you do not need to provide a key.

The username value is the login user name associated with the specified encryption. You must enter the username in the same case you used when you added the user. To see the case of the username, enter the show users command.

Default
no encryption
Format
username snmpv3 encryption username {none | des[key]}
Mode
Global Config

2.8.14.1 no username snmpv3 encryption
This command sets the encryption protocol to none. The username is the login user name for which the specified encryption protocol will be used.

Format
no username snmpv3 encryption username
Mode
Global Config

2.8.15 username snmpv3 encryption encrypted
This command specifies the des encryption protocol and the required encryption key for the specified user. The encryption key must be 8 to 64 characters long.

Default
no encryption
Format
username snmpv3 encryption encrypted username des key
Mode
Global Config

2.8.16 show users
This command displays the configured user names and their settings. The show users command displays truncated user names. Use the show users long command to display the complete usernames. The show users command is only available for users with Level 15 privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format
show users
Mode
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The name the user enters to login using the serial port, Telnet or Web.</td>
</tr>
</tbody>
</table>
2.8.17  show users long

This command displays the complete usernames of the configured users on the switch.

Format       show users long
Mode         Privileged EXEC

Example: The following shows an example of the command.

(switch) #show users long
User Name     ------------
admin         
guest         
test1111test1111test1111test1111

2.8.18  show users accounts

This command displays the local user status with respect to user account lockout and password aging. This command displays truncated user names. Use the show users long command to display the complete usernames.

Format       show users accounts [detail]
Mode         Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The local user account’s user name.</td>
</tr>
<tr>
<td>Access Level</td>
<td>The user’s access level (1 for non-privilege (switch&gt;prompt) or 15 for highest privilege (switch# prompt)).</td>
</tr>
<tr>
<td>Password Aging</td>
<td>Number of days, since the password was configured, until the password expires.</td>
</tr>
<tr>
<td>Password Expiry Date</td>
<td>The current password expiration date in date format.</td>
</tr>
<tr>
<td>Lockout</td>
<td>Indicates whether the user account is locked out (true or false).</td>
</tr>
</tbody>
</table>

If the detail keyword is included, the following additional fields display.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Override Complexity Check</td>
<td>Displays the user’s Password override complexity check status. By default it is disabled.</td>
</tr>
<tr>
<td>Password Strength</td>
<td>Displays the user password’s strength (Strong or Weak). This field is displayed only if the Password Strength feature is enabled.</td>
</tr>
</tbody>
</table>
Example: The following example displays information about the local user database.

(switch)#show users accounts

<table>
<thead>
<tr>
<th>UserName</th>
<th>Privilege</th>
<th>Password Aging</th>
<th>Password Expiry</th>
<th>Lockout</th>
<th>Lockout</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>15</td>
<td>---</td>
<td>---</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>guest</td>
<td>1</td>
<td>---</td>
<td>---</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>

console#show users accounts detail

<table>
<thead>
<tr>
<th>UserName</th>
<th>Privilege</th>
<th>Password Aging</th>
<th>Password Expiry</th>
<th>Lockout</th>
<th>Override Complexity Check</th>
<th>Password Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>15</td>
<td>---</td>
<td>---</td>
<td>False</td>
<td>Disable</td>
<td>-</td>
</tr>
<tr>
<td>guest</td>
<td>1</td>
<td>---</td>
<td>---</td>
<td>False</td>
<td>Disable</td>
<td>-</td>
</tr>
</tbody>
</table>

2.8.19 show users login-history [long]

Use this command to display information about the login history of users.

Format: show users login-history [long]
Mode: Privileged EXEC

2.8.20 show users login-history [username]

Use this command to display information about the login history of users.

Format: show users login-history [username name]
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the user. Range: 1-20 characters.</td>
</tr>
</tbody>
</table>

Example: The following example shows user login history outputs.

Console>show users login-history

<table>
<thead>
<tr>
<th>Login Time</th>
<th>Username</th>
<th>Protocol</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 19 2005 08:23:48</td>
<td>Bob</td>
<td>Serial</td>
<td></td>
</tr>
<tr>
<td>Jan 19 2005 08:29:29</td>
<td>Robert</td>
<td>HTTP</td>
<td>172.16.0.8</td>
</tr>
<tr>
<td>Jan 19 2005 08:42:31</td>
<td>John</td>
<td>SSH</td>
<td>172.16.0.1</td>
</tr>
<tr>
<td>Jan 19 2005 08:49:52</td>
<td>Betty</td>
<td>Telnet</td>
<td>172.16.1.7</td>
</tr>
</tbody>
</table>
2.8.21 login authentication

Use this command to specify the login authentication method list for a line (console, telnet, or SSH). The default configuration uses the default set with the command `aaa authentication login`.

**Format**

```
login authentication {default | list-name}
```

**Mode**

Line Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Uses the default list created with the <code>aaa authentication login</code> command.</td>
</tr>
<tr>
<td>list-name</td>
<td>Uses the indicated list created with the <code>aaa authentication login</code> command.</td>
</tr>
</tbody>
</table>

**Example:** The following example specifies the default authentication method for a console.

```
(switch) (config) line console
(switch) (config-line)# login authentication default
```

2.8.21.1 no login authentication

Use this command to return to the default specified by the `authentication login` command.

2.8.22 password

This command allows the currently logged in user to change his or her password without having Level 15 privileges.

**Format**

```
password
```

**Mode**

User EXEC

**Example:** The following is an example of the command.

```
console>password
Enter old password:********
Enter new password:********
Confirm new password:********
```

2.8.23 password (Line Configuration)

Use the `password` command in Line Configuration mode to specify a password on a line. The default configuration is no password is specified.

**Format**

```
password [password [encrypted]]
```

**Mode**

Line Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>Password for this level. Range: 8-64 characters</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypted password to be entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.</td>
</tr>
</tbody>
</table>
**Example:** The following example specifies a password `mcmxxyyy` on a line.

```
(switch)(config-line)# password mcmxxyyy
```

**Example:** The following is another example of the command.

```
(Switching)(Config-line)# password testtest
```

```
(Switching) (Config-line)# password
```

```
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b1b7ab91be84
2278e5e970dbfc62d16dcd13c0b864 encrypted
```

```
(Switching) (Config-line)# password
```

```
Enter new password:********
Confirm new password:********
```

### 2.8.23.1  no password (Line Configuration)
Use this command to remove the password on a line.

<table>
<thead>
<tr>
<th>Format</th>
<th>no password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Line Config</td>
</tr>
</tbody>
</table>

### 2.8.24  password (User EXEC)
Use this command to allow a user to change the password for only that user. This command should be used after the password has aged. The user is prompted to enter the old password and the new password.

<table>
<thead>
<tr>
<th>Format</th>
<th>password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>User EXEC</td>
</tr>
</tbody>
</table>

**Example:** The following example shows the prompt sequence for executing the password command.

```
(switch)>password
```

```
Enter old password:********
Enter new password:********
Confirm new password:********
```

### 2.8.25  password (aaa IAS User Config)
This command is used to configure a password for a user. An optional parameter `[encrypted]` is provided to indicate that the password given to the command is already preencrypted.

<table>
<thead>
<tr>
<th>Format</th>
<th>password password [encrypted]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>aaa IAS User Config</td>
</tr>
</tbody>
</table>
2.8.25.1  no password (aaa IAS User Config)

This command is used to clear the password of a user.

**Format**  
no password

**Mode**  
aaa IAS User Config

**Example:** The following shows an example of the command.

```
(Switching) #
(Switching) #configure
(Switching) (Config)#aaa ias-user username client-1
(Switching) (Config-aaa-ias-User)#password client123
(Switching) (Config-aaa-ias-User)#no password
```

**Example:** The following is an example of adding a MAB Client to the Internal user database.

```
(Switching) #
(Switching) #configure
(Switching) (Config)#aaa ias-user username 1f3ccb1157
(Switching) (Config-aaa-ias-User)#password 1f3ccb1157
(Switching) (Config-aaa-ias-User)#exit
(Switching) (Config)#
```

2.8.26  enable password (Privileged EXEC)

Use the `enable password` configuration command to set a local password to control access to the privileged EXEC mode.

**Format**  
enable password [password [encrypted]]

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>Password string. Range: 8-64 characters.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypted password you entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.</td>
</tr>
</tbody>
</table>

**Example:** The following shows an example of the command.

```
(Switching) #enable password testtest

(Switching) #enable password e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cda1b1b7ab91be842278e9e970dbfc62d16cd13c0b864 encrypted

(Switching) #enable password

Enter old password:********

Enter new password:********

Confirm new password:********
```
2.8.26.1 no enable password (Privileged EXEC)

Use the no enable password command to remove the password requirement.

Format: 
```
no enable password
```

Mode: Privileged EXEC

2.8.27 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

2.8.27.1 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

2.8.28 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

2.8.28.1 no passwords history

Use this command to set the password history to the default value.

Format: 
```
no passwords history
```

Mode: Global Config

2.8.29 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
2.8.29.1 no passwords aging
Use this command to set the password aging to the default value.

Format: no passwords aging
Mode: Global Config

2.8.30 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 Level 15 access can reactivate 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

2.8.30.1 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

2.8.31 passwords strength-check
Use this command to enable the password strength feature. It is used to verify the strength of a password during configuration.

Default: Disable
Format: passwords strength-check
Mode: Global Config

2.8.31.1 no passwords strength-check
Use this command to set the password strength checking to the default value.

Format: no passwords strength-check
Mode: Global Config

2.8.32 passwords strength maximum consecutive-characters
Use this command to set the maximum number of consecutive characters to be used in password strength. The valid range is 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default: 0
Format: passwords strength maximum consecutive-characters 0-15
Mode: Global Config
2.8.33 passwords strength maximum repeated-characters
Use this command to set the maximum number of repeated characters to be used in password strength. The valid range is 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default 0
Format passwords strength maximum consecutive-characters \texttt{0-15}
Mode Global Config

2.8.34 passwords strength minimum uppercase-letters
Use this command to enforce a minimum number of uppercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default 2
Format passwords strength minimum uppercase-letters
Mode Global Config

2.8.34.1 no passwords strength minimum uppercase-letters
Use this command to reset the minimum uppercase letters required in a password to the default value.

Format no passwords minimum uppercase-letter
Mode Global Config

2.8.35 passwords strength minimum lowercase-letters
Use this command to enforce a minimum number of lowercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default 2
Format passwords strength minimum lowercase-letters
Mode Global Config

2.8.35.1 no passwords strength minimum lowercase-letters
Use this command to reset the minimum lower letters required in a password to the default value.

Format no passwords minimum lowercase-letter
Mode Global Config

2.8.36 passwords strength minimum numeric-characters
Use this command to enforce a minimum number of numeric characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default 2
Format passwords strength minimum numeric-characters
Mode Global Config
2.8.36.1  no passwords strength minimum numeric-characters
Use this command to reset the minimum numeric characters required in a password to the default value.

Format  no passwords minimum numeric-characters
Mode    Global Config

2.8.37  passwords strength minimum special-characters
Use this command to enforce a minimum number of special characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default  2
Format    passwords strength minimum special-characters
Mode      Global Config

2.8.37.1  no passwords strength minimum special-characters
Use this command to reset the minimum special characters required in a password to the default value.

Format    no passwords minimum special-characters
Mode      Global Config

2.8.38  passwords strength minimum character-classes
Use this command to enforce a minimum number of character classes that a password should contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. The valid range is 0-4. The default is 4.

Default  4
Format    passwords strength minimum character-classes
Mode      Global Config

2.8.38.1  no passwords strength minimum character-classes
Use this command to reset the minimum number of character classes required in a password to the default value.

Format    no passwords minimum character-classes
Mode      Global Config

2.8.39  passwords strength exclude-keyword
Use this command to exclude the specified keyword while configuring the password. The password does not accept the keyword in any form (in between the string, case insensitive and reverse) as a substring. User can configure up to a maximum of 3 keywords.

Format    passwords strength exclude-keyword <keyword>
Mode      Global Config
2.8.39.1  no passwords strength exclude-keyword

Use this command to reset the restriction for the specified keyword or all the keywords configured.

**Format**

no passwords exclude-keyword [keyword]

**Mode**

Global Config

2.8.40  show passwords configuration

Use this command to display the configured password management settings.

**Format**

show passwords configuration

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Password Length</td>
<td>Minimum number of characters required when changing passwords.</td>
</tr>
<tr>
<td>Password History</td>
<td>Number of passwords to store for reuse prevention.</td>
</tr>
<tr>
<td>Password Aging</td>
<td>Length in days that a password is valid.</td>
</tr>
<tr>
<td>Lockout Attempts</td>
<td>Number of failed password login attempts before lockout.</td>
</tr>
<tr>
<td>Minimum Password Uppercase Letters</td>
<td>Minimum number of uppercase characters required when configuring passwords.</td>
</tr>
<tr>
<td>Minimum Password Lowercase Letters</td>
<td>Minimum number of lowercase characters required when configuring passwords.</td>
</tr>
<tr>
<td>Minimum Password Numeric Characters</td>
<td>Minimum number of numeric characters required when configuring passwords.</td>
</tr>
<tr>
<td>Maximum Password Consecutive Characters</td>
<td>Maximum number of consecutive characters required that the password should contain when configuring passwords.</td>
</tr>
<tr>
<td>Maximum Password Repeated Characters</td>
<td>Maximum number of repetition of characters that the password should contain when configuring passwords.</td>
</tr>
<tr>
<td>Minimum Password Character Classes</td>
<td>Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.</td>
</tr>
<tr>
<td>Password Exclude-Keywords</td>
<td>The set of keywords to be excluded from the configured password when strength checking is enabled.</td>
</tr>
</tbody>
</table>

2.8.41  show passwords result

Use this command to display the last password set result information.

**Format**

show passwords result

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last User Whose Password Is Set</td>
<td>Shows the name of the user with the most recently set password.</td>
</tr>
<tr>
<td>Password Strength Check</td>
<td>Shows whether password strength checking is enabled.</td>
</tr>
<tr>
<td>Last Password Set Result</td>
<td>Shows whether the attempt to set a password was successful. If the attempt failed, the reason for the failure is included.</td>
</tr>
</tbody>
</table>
2.8.42 aaa ias-user username

The Internal Authentication Server (IAS) database is a dedicated internal database used for local authentication of users for network access through the IEEE 802.1X feature.

Use the `aaa ias-user username` command in Global Config mode to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

**Format**
```
aaa ias-user username user
```

**Mode**
Global Config

2.8.42.1 no aaa ias-user username

Use this command to remove the specified user from the internal user database.

**Format**
```
oo aaa ias-user username user
```

**Mode**
Global Config

**Example:** The following shows an example of the command.
```
(FASTPATH Routing) #
(FASTPATH Routing) #configure
(FASTPATH Routing) (Config)#aaa ias-user username client-1
(FASTPATH Routing) (Config-aaa-ias-User)#exit
(FASTPATH Routing) (Config)#no aaa ias-user username client-1
(FASTPATH Routing) (Config)#
```

2.8.43 aaa session-id

Use this command in Global Config mode to specify if the same session-id is used for Authentication, Authorization and Accounting service type within a session.

**Default**
common

**Format**
```
aaa session-id [common | unique]
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common</td>
<td>Use the same session-id for all AAA Service types.</td>
</tr>
<tr>
<td>unique</td>
<td>Use a unique session-id for all AAA Service types.</td>
</tr>
</tbody>
</table>

2.8.43.1 no aaa session-id

Use this command in Global Config mode to reset the aaa session-id behavior to the default.

**Format**
```
oo aaa session-id [unique]
```

**Mode**
Global Config

2.8.44 aaa accounting

Use this command in Global Config mode to create an accounting method list for user EXEC sessions, user-executed commands, or DOT1X. This list is identified by default or a user-specified list_name. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end (start-stop) or only at the end (stop-only). If none is specified, then accounting is disabled for the specified list. If tacacs is specified as the accounting method, accounting records are notified to a TACACS+ server. If radius is the specified accounting method, accounting records are notified to a RADIUS server.
Please note the following:

- A maximum of five Accounting Method lists can be created for each exec and commands type.
- Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.
- The same list-name can be used for both exec and commands accounting type.
- AAA Accounting for commands with RADIUS as the accounting method is not supported.
- Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.
- RADIUS is the only accounting method type supported for DOT1X accounting.

**Format**
```
aaa accounting {exec | commands | dot1x} {default | list_name} {start-stop | stop-only | none} method1 [method2...]
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exec</td>
<td>Provides accounting for a user EXEC terminal sessions.</td>
</tr>
<tr>
<td>commands</td>
<td>Provides accounting for all user executed commands.</td>
</tr>
<tr>
<td>dot1x</td>
<td>Provides accounting for DOT1X user commands.</td>
</tr>
<tr>
<td>default</td>
<td>The default list of methods for accounting services.</td>
</tr>
<tr>
<td>list-name</td>
<td>Character string used to name the list of accounting methods.</td>
</tr>
<tr>
<td>start-stop</td>
<td>Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process.</td>
</tr>
<tr>
<td>stop-only</td>
<td>Sends a stop accounting notice at the end of the requested user process.</td>
</tr>
<tr>
<td>none</td>
<td>Disables accounting services on this line.</td>
</tr>
<tr>
<td>method</td>
<td>Use either TACACS or radius server for accounting purposes.</td>
</tr>
</tbody>
</table>

**Example:** The following shows an example of the command.

```
(Routing) #
(Routing) #configure
(Routing) #aaa accounting commands default stop-only tacacs
(Routing) #aaa accounting exec default start-stop radius
(Routing) #aaa accounting dot1x default start-stop radius
(Routing) #aaa accounting dot1x default none
(Routing) #exit
```

For the same set of accounting type and list name, the administrator can change the record type, or the methods list, without having to first delete the previous configuration.

```
(Routing) #
(Routing) #configure
(Routing) #aaa accounting exec ExecList stop-only tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs radius
```

The first aaa command creates a method list for exec sessions with the name ExecList, with record-type as stop-only and the method as TACACS+. The second command changes the record type to start-stop from stop-only for the same method list. The third command, for the same list changes the methods list to (tacacs,radius) from (tacacs).
2.8.44.1 no aaa accounting
This command deletes the accounting method list.

Format
no aaa accounting {exec | commands | dot1x} {default | list_name default}

Mode
Global Config

Example: The following shows an example of the command.
(Routing) #
(Routing) #configure
(Routing) #aaa accounting commands userCmdAudit stop-only tacacs radius
(Routing) #no aaa accounting commands userCmdAudit
(Routing) #exit

2.8.45 password (AAA IAS User Configuration)
Use this command to specify a password for a user in the IAS database. An optional parameter encrypted is provided to indicate that the password given to the command is already preencrypted.

Format
password password [encrypted]

Mode
AAA IAS User Config

Parameter | Definition
---|---
password | Password for this level. Range: 8-64 characters
encrypted | Encrypted password to be entered, copied from another switch configuration.

2.8.45.1 no password (AAA IAS User Configuration)
Use this command to clear the password of a user.

Format
no password

Mode
AAA IAS User Config

Example: The following shows an example of the command.
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username client-1
(Routing) (Config-aaa-ias-User)#password client123
(Routing) (Config-aaa-ias-User)#no password

Example: The following is an example of adding a MAB Client to the Internal user database.
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username 1f3ccb1157
(Routing) (Config-aaa-ias-User)#password 1f3ccb1157
(Routing) (Config-aaa-ias-User)#exit
(Routing) (Config)#

2.8.46 clear aaa ias-users
Use this command to remove all users from the IAS database.

Format
clear aaa ias-users

Mode
Privileged EXEC
Example: The following is an example of the command.

(Routing) #
(Routing) #clear aaa ias-users
(Routing) #

2.8.47 show aaa ias-users

Use this command to display configured IAS users and their attributes. Passwords configured are not shown in the show command output.

Format: show aaa ias-users [username]
Mode: Privileged EXEC

Example: The following is an example of the command.

(Routing) #
(Routing) #show aaa ias-users

UserName
----------------
Client-1
Client-2

Example: Following are the IAS configuration commands shown in the output of show running-config command. Passwords shown in the command output are always encrypted.

aaa ias-user username client-1
password a45c74fdf50a558a2b5cf05573cd633bac2c6c598d54497ad4c46104918f2c encrypted
exit

2.8.48 accounting

Use this command in Line Configuration mode to apply the accounting method list to a line config (console/telnet/ssh).
Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

Format: accounting {exec | commands} {default | listname}
Mode: Line Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exec</td>
<td>Causes accounting for an EXEC session.</td>
</tr>
<tr>
<td>commands</td>
<td>This causes accounting for each command execution attempt. If a user is enabling accounting for exec mode for the current line-configuration type, the user will be logged out.</td>
</tr>
<tr>
<td>default</td>
<td>The default Accounting List</td>
</tr>
<tr>
<td>listname</td>
<td>Enter a string of not more than 15 characters.</td>
</tr>
</tbody>
</table>

Example: The following is a example of the command.

(Routing) #
(Routing) #configure
(Routing) (Config)#line telnet
(Routing)(Config-line)# accounting exec default
(Routing) #exit
2.8.48.1 no accounting

Use this command to remove accounting from a Line Configuration mode.

Format  no accounting \{exec|commands\}
Mode     Line Configuration

2.8.49 show accounting

Use this command to display ordered methods for accounting lists.

Format  show accounting
Mode     Privileged EXEC

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

(Routing) # show accounting
Number of Accounting Notifications sent at beginning of an EXEC session: 0
Errors when sending Accounting Notifications beginning of an EXEC session: 0
Number of Accounting Notifications at end of an EXEC session: 0
Errors when sending Accounting Notifications at end of an EXEC session: 0
Number of Accounting Notifications sent at beginning of a command execution: 0
Errors when sending Accounting Notifications at beginning of a command execution: 0
Number of Accounting Notifications sent at end of a command execution: 0
Errors when sending Accounting Notifications at end of a command execution: 0

2.8.50 show accounting methods

Use this command to display configured accounting method lists.

Format  show accounting methods
Mode     Privileged EXEC

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

(Routing) #
(Routing) # show accounting methods

<table>
<thead>
<tr>
<th>Acct Type</th>
<th>Method Name</th>
<th>Record Type</th>
<th>Method Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec</td>
<td>dfltExecList</td>
<td>start-stop</td>
<td>TACACS</td>
</tr>
<tr>
<td>Commands</td>
<td>dflt_CmdsList</td>
<td>stop-only</td>
<td>TACACS</td>
</tr>
<tr>
<td>Commands</td>
<td>User_CmdAudit</td>
<td>start-stop</td>
<td>TACACS</td>
</tr>
<tr>
<td>DOT1X</td>
<td>dflt_Dot1xList</td>
<td>start-stop</td>
<td>radius</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Line</th>
<th>EXEC Method List</th>
<th>Command Method List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>dfltExecList</td>
<td>dflt_CmdsList</td>
</tr>
<tr>
<td>Telnet</td>
<td>dfltExecList</td>
<td>dflt_CmdsList</td>
</tr>
<tr>
<td>SSH</td>
<td>dfltExecList</td>
<td>User_CmdAudit</td>
</tr>
</tbody>
</table>

2.8.51 clear accounting statistics

This command clears the accounting statistics.

Format  clear accounting statistics
Mode     Privileged EXEC
2.8.52  show domain-name

This command displays the configured domain-name.

**Format**

show domain-name

**Mode**

Privileged EXEC

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

(Routing) #
(Routing) #show domain-name

Domain : Enable
Domain-name : abc

2.9  SNMP Commands

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

2.9.1  snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The parameters `name`, `loc` and `con` can be up to 255 characters in length.

**Default**

none

**Format**

snmp-server {sysname name | location loc | contact con}

**Mode**

Global Config

To clear the snmp-server, enter an empty string in quotes. For example, `snmp-server {sysname " "}` clears the system name.

2.9.2  snmp-server community

This command adds (and names) a new SNMP community, and optionally sets the access mode, allowed IP address, and create a view for the community.

**Default**

Two communities are created by default:
- `public`, with read-only permissions, a view name of Default, and allows access from all IP addresses.
- `private`, with read/write permissions, a view name of Default, and allows access from all IP addresses.

**Format**

snmp-server community community-string [{ro | rw | su}] [ipaddress ip-address] [view view-name]

**Mode**

Global Config

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.
2.9.2.1 no snmp-server community

This command removes this community name from the table. The `name` is the community name to be deleted.

**Format**

```
no snmp-server community community-name
```

**Mode**

Global Config

2.9.3 snmp-server community-group

This command configures a community access string to permit access via the SNMPv1 and SNMPv2c protocols.

**Format**

```
snmp-server community-group community-string group-name [ipaddress ipaddress]
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community-string</td>
<td>The community which is created and then associated with the group. The range is 1 to 20 characters.</td>
</tr>
<tr>
<td>group-name</td>
<td>The name of the group that the community is associated with. The range is 1 to 30 characters.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Optionally, the IPv4 address that the community may be accessed from.</td>
</tr>
</tbody>
</table>

2.9.4 snmp-server enable traps violation

The Port MAC locking component interprets this command and configures violation action to send an SNMP trap with default trap frequency of 30 seconds. The Global command configures the trap violation mode across all interfaces valid for port-security. There is no global trap mode as such.

**Default**

```
disabled
```

**Format**

```
snmp-server enable traps violation
```

**Mode**

- Global Config
- Interface Config

---

**Notice**

For other port security commands, see “Port Security Commands” on page 470.
2.9.4.1  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

2.9.5     snmp-server enable traps
This command enables the Authentication Flag.
Default  enabled
Format    snmp-server enable traps
Mode      Global Config

2.9.5.1  no snmp-server enable traps
This command disables the Authentication Flag.
Format    no snmp-server enable traps
Mode      Global Config

2.9.6     snmp-server enable traps all
This command enables all traps.
Default   enabled
Format    snmp-server enable traps all
Mode      Global Config

2.9.6.1  no snmp-server enable traps
This command disables all traps.
Format    no snmp-server enable traps all
Mode      Global Config

2.9.7     snmp-server port
This command configures the UDP port number on which the SNMP server listens for requests.
Default   161
Format    snmp-server port 1025-65535
Mode      Privileged EXEC
2.9.7.1 no snmp-server port
This command restores the SNMP server listen port to its factory default value.

Format no snmp-server port
Mode Privileged EXEC

2.9.8 snmp trap link-status
This command enables link status traps on an interface or range of interfaces.

Format snmp trap link-status
Mode Interface Config

2.9.8.1 no snmp trap link-status
This command disables link status traps by interface.

Format no snmp trap link-status
Mode Interface Config

2.9.9 snmp trap link-status all
This command enables link status traps for all interfaces.

Format snmp trap link-status all
Mode Global Config

2.9.9.1 no snmp trap link-status all
This command disables link status traps for all interfaces.

Format no snmp trap link-status all
Mode Global Config
2.9.10  snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See “show snmp” on page 81.

Default enabled
Format snmp-server enable traps linkmode
Mode Global Config

2.9.10.1  no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format no snmp-server enable traps linkmode
Mode Global Config

2.9.11  snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default enabled
Format snmp-server enable traps multiusers
Mode Global Config

2.9.11.1  no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format no snmp-server enable traps multiusers
Mode Global Config

2.9.12  snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default enabled
Format snmp-server enable traps stpmode
Mode Global Config
2.9.12.1 no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

**Format**
```
no snmp-server enable traps stpmode
```

**Mode**
Global Config

2.9.13 snmp-server engineID local

This command configures the SNMP engine ID on the local device.

**Default**
The engineID is configured automatically, based on the device MAC address.

**Format**
```
snmp-server engineID local {engineid-string|default}
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>engineid-string</td>
<td>A hexadecimal string identifying the engine-id, used for localizing configuration. Engine-id must be an even length in the range of 6 to 32 hexadecimal characters.</td>
</tr>
<tr>
<td>default</td>
<td>Sets the engine-id to the default string, based on the device MAC address.</td>
</tr>
<tr>
<td>ip</td>
<td>The command is extended by KONTRON to select a RFC 3411 defined algorithm using a specified IP address (ip). The IP address must be specified as string. A RFC 3411 related prefix (5 octets) is added. Note that the show command shows the engine-id always hexadecimal.</td>
</tr>
<tr>
<td>text</td>
<td>The command is extended by KONTRON to select a RFC 3411 defined algorithm using a specified text (text). The text must be specified as string, it may be quoted to allow spaces, maximum length is 27 characters. A RFC 3411 related prefix (5 octets) is added. Note that the show command shows the engine-id always hexadecimal.</td>
</tr>
</tbody>
</table>

⚠️ CAUTION ⚠️
Changing the engine-id will invalidate all SNMP configuration that exists on the box.

2.9.13.1 no snmp-server engineID local

This command removes the specified engine ID.

**Default**
The engineID is configured automatically, based on the device MAC address.

**Format**
```
no snmp-server engineID local
```

**Mode**
Global Config

2.9.14 snmp-server filter

This command creates a filter entry for use in limiting which traps will be sent to a host.

**Default**
No filters are created by default.

**Format**
```
snmp-server filter filtername oid-tree {included|excluded}
```

**Mode**
Global Config
2.9.14.1 no snmp-server filter
This command removes the specified filter.

Default
No filters are created by default.

Format
snmp-server filter filtername [oid-tree]

Mode
Global Config

2.9.15 snmp-server group
This command creates an SNMP access group.

Default
Generic groups are created for all versions and privileges using the default views.

Format
snmp-server group group-name {v1 | v2c | v3 {noauth | auth | priv}} [context context-name] [read read-view] [write write-view] [notify notify-view]

Mode
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filtername</td>
<td>The label for the filter being created. The range is 1 to 30 characters.</td>
</tr>
<tr>
<td>oid-tree</td>
<td>The OID subtree to include or exclude from the filter. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).</td>
</tr>
<tr>
<td>included</td>
<td>The tree is included in the filter.</td>
</tr>
<tr>
<td>excluded</td>
<td>The tree is excluded from the filter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-name</td>
<td>The group name to be used when configuring communities or users. The range is 1 to 30 characters.</td>
</tr>
<tr>
<td>v1</td>
<td>This group can only access via SNMPv1.</td>
</tr>
<tr>
<td>v2</td>
<td>This group can only access via SNMPv2c.</td>
</tr>
<tr>
<td>v3</td>
<td>This group can only access via SNMPv3.</td>
</tr>
<tr>
<td>noauth</td>
<td>This group can be accessed only when not using Authentication or Encryption. Applicable only if SNMPv3 is selected.</td>
</tr>
<tr>
<td>auth</td>
<td>This group can be accessed only when using Authentication but not Encryption. Applicable only if SNMPv3 is selected.</td>
</tr>
<tr>
<td>priv</td>
<td>This group can be accessed only when using both Authentication and Encryption. Applicable only if SNMPv3 is selected.</td>
</tr>
<tr>
<td>context-name</td>
<td>The SNMPv3 context used during access. Applicable only if SNMPv3 is selected.</td>
</tr>
<tr>
<td>read-view</td>
<td>The view this group will use during GET requests. The range is 1 to 30 characters.</td>
</tr>
<tr>
<td>write-view</td>
<td>The view this group will use during SET requests. The range is 1 to 30 characters.</td>
</tr>
<tr>
<td>notify-view</td>
<td>The view this group will use when sending out traps. The range is 1 to 30 characters.</td>
</tr>
</tbody>
</table>
2.9.15.1 no snmp-server group

This command removes the specified group.

Format:
```
no snmp-server group group-name {v1|v2c| 3 {noauth|auth|priv}} [context context-name]
```

Mode: Global Config

2.9.16 snmp-server host

This command configures traps to be sent to the specified host.

Default: No default hosts are configured.

Format:
```
snmp-server host host-addr {informs [timeout seconds] [retries retries]|traps version {1 | 2c }} community-string [udp-port port] [filter filter-name]
```

Mode: Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-addr</td>
<td>The IPv4 or IPv6 address of the host to send the trap or inform to.</td>
</tr>
<tr>
<td>traps</td>
<td>Send SNMP traps to the host. This option is selected by default.</td>
</tr>
<tr>
<td>version 1</td>
<td>Sends SNMPv1 traps. This option is not available if informs is selected.</td>
</tr>
<tr>
<td>version 2</td>
<td>Sends SNMPv2c traps. This option is not available if informs is selected.</td>
</tr>
<tr>
<td>informs</td>
<td>Send SNMPv2 informs to the host.</td>
</tr>
<tr>
<td>seconds</td>
<td>The number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.</td>
</tr>
<tr>
<td>retries</td>
<td>The number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.</td>
</tr>
<tr>
<td>community-string</td>
<td>Community string sent as part of the notification. The range is 1 to 20 characters.</td>
</tr>
<tr>
<td>port</td>
<td>The SNMP Trap receiver port. The default is port 162.</td>
</tr>
<tr>
<td>filter-name</td>
<td>The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.</td>
</tr>
</tbody>
</table>

2.9.16.1 no snmp-server host

This command removes the specified host entry.

Format:
```
no snmp-server host host-addr [traps|informs]
```

Mode: Global Config

2.9.17 snmp-server user

This command creates an SNMPv3 user for access to the system.

Default: No default users are created.

Format:
```
snmp-server user username groupname [remote engineid-string] [ {auth-md5 password | auth-sha password | auth-md5-key md5-key | auth-sha-key sha-key} [priv-des password | priv-des-key des-key]]
```

Mode: Global Config
2.9.17.1 no snmp-server user

This command removes the specified SNMPv3 user.

**Format**

```
no snmp-server user username
```

**Mode**

Global Config

2.9.18 snmp-server view

This command creates or modifies an existing view entry that is used by groups to determine which objects can be accessed by a community or user.

**Default**

Views are created by default to provide access to the default groups.

**Format**

```
snmp-server viewname oid-tree {included|excluded}
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>viewname</td>
<td>The label for the view being created. The range is 1 to 30 characters.</td>
</tr>
<tr>
<td>oid-tree</td>
<td>The OID subtree to include or exclude from the view. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).</td>
</tr>
<tr>
<td>included</td>
<td>The tree is included in the view.</td>
</tr>
<tr>
<td>excluded</td>
<td>The tree is excluded from the view.</td>
</tr>
</tbody>
</table>
2.9.18.1  no snmp-server view

This command removes the specified view.

**Format**

```
no snmp-server view viewname [oid-tree]
```

**Mode**

Global Config

---

2.9.19  snmp-server v3-host

This command configures traps to be sent to the specified host.

**Default**

No default hosts are configured.

**Format**

```
snmp-server v3-host host-addr username [traps | informs [timeout seconds] [retries retries]] [auth | noauth | priv] [udpport port] [filter filtername]
```

**Mode**

Global Config

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-addr</td>
<td>The IPv4 or IPv6 address of the host to send the trap or inform to.</td>
</tr>
<tr>
<td>user-name</td>
<td>User used to send a Trap or Inform message. This user must be associated with a group that supports the version and access method. The range is 1 to 30 characters.</td>
</tr>
<tr>
<td>traps</td>
<td>Send SNMP traps to the host. This is the default option.</td>
</tr>
<tr>
<td>informs</td>
<td>Send SNMP informs to the host.</td>
</tr>
<tr>
<td>seconds</td>
<td>Number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.</td>
</tr>
<tr>
<td>retries</td>
<td>Number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.</td>
</tr>
<tr>
<td>auth</td>
<td>Enables authentication but not encryption.</td>
</tr>
<tr>
<td>noauth</td>
<td>No authentication or encryption. This is the default.</td>
</tr>
<tr>
<td>priv</td>
<td>Enables authentication and encryption.</td>
</tr>
<tr>
<td>port</td>
<td>The SNMP Trap receiver port. This value defaults to port 162.</td>
</tr>
<tr>
<td>filter-name</td>
<td>The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.</td>
</tr>
</tbody>
</table>

---

2.9.20  snmptrap source-interface

Use this command in Global Configuration mode to configure the global source-interface (Source IP address) for all SNMP communication between the SNMP client and the server.

**Format**

```
snmptrap source-interface {slot/port | loopback loopback-id|tunnel tunnel-id|vlan vlan-id}
```

**Mode**

Global Configuration

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>The unit identifier assigned to the switch.</td>
</tr>
<tr>
<td>loopback-id</td>
<td>Configures the loopback interface. The range of the loopback ID is 0 to 7.</td>
</tr>
<tr>
<td>tunnel-id</td>
<td>Configures the IPv6 tunnel interface. The range of the tunnel ID is 0 to 7.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.</td>
</tr>
</tbody>
</table>
2.9.20.1 no snmptrap source-interface
Use this command in Global Configuration mode to remove the global source-interface (Source IP selection) for all SNMP communication between the SNMP client and the server.

Format: no snmptrap source-interface
Mode: Global Configuration

2.9.21 snmptrap ipaddr 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.

This command does not support a “no” form.

Format: snmptrap ipaddr snmpversion name snmpversion
Mode: Global Configuration

2.9.22 snmptrap ip6addr 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.

This command does not support a “no” form.

Format: snmptrap ip6addr snmpversion name snmpversion
Mode: Global Configuration

2.9.23 show snmp
This command displays the current SNMP configuration.

Format: show snmp
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Table:</td>
<td></td>
</tr>
<tr>
<td>Community-String</td>
<td>The community string for the entry. This is used by SNMPv1 and SNMPv2 protocols to access the switch.</td>
</tr>
<tr>
<td>Community-Access</td>
<td>The type of access the community has:</td>
</tr>
<tr>
<td></td>
<td>• Read only</td>
</tr>
<tr>
<td></td>
<td>• Read write</td>
</tr>
<tr>
<td></td>
<td>• su</td>
</tr>
<tr>
<td>View Name</td>
<td>The view this community has access to.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Access to this community is limited to this IP address.</td>
</tr>
</tbody>
</table>
2.9.24 show snmp engineID

This command displays the currently configured SNMP engineID.

**Format**

```
show snmp engineID
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local SNMP EngineID</td>
<td>The current configuration of the displayed SNMP engineID.</td>
</tr>
</tbody>
</table>

2.9.25 show snmp filters

This command displays the configured filters used when sending traps.

**Format**

```
show snmp filters [filtername]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The filter name for this entry.</td>
</tr>
<tr>
<td>OID Tree</td>
<td>The OID tree this entry will include or exclude.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates if this entry includes or excludes the OID Tree.</td>
</tr>
</tbody>
</table>

2.9.26 show snmp group

This command displays the configured groups.

**Format**

```
show snmp group [groupname]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the group.</td>
</tr>
<tr>
<td>Security Model</td>
<td>Indicates which protocol can access the system via this group.</td>
</tr>
</tbody>
</table>
2.9.27  

```
This command displays the current SNMP server user configuration. The command is extended by Kontron (parameter 'sysinfo') to display additionally snmp-server system information. This consists of the name, the physical location of the switch or the organisation responsible for network. All parameters are listed for 'all'. This information is provided for the SNMP in the standard MIB-2 in OIDs “sysName”, “sysLocation” and ‘sysContact’.
```

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

(Routing)# show snmp-server
SNMP Server Port......................... 161
```

2.9.28  

```
Use this command in Privileged EXEC mode to display the configured global source-interface (Source IP address) details used for an SNMP client.
```

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

(Routing)# show snmp source-interface
SNMP trap Client Source Interface.............. (not configured)
```

2.9.29  

```
This command displays the currently configured SNMPv3 users.
```

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the user.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The group that defines the SNMPv3 access parameters.</td>
</tr>
<tr>
<td>Auth Method</td>
<td>The authentication algorithm configured for this user.</td>
</tr>
<tr>
<td>Privilege Method</td>
<td>The encryption algorithm configured for this user.</td>
</tr>
<tr>
<td>Remote Engine ID</td>
<td>The engineID for the user defined on the client machine.</td>
</tr>
</tbody>
</table>
2.9.30 show snmp views

This command displays the currently configured views.

**Format**

```
show snmp views [viewname]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The view name for this entry.</td>
</tr>
<tr>
<td>OID Tree</td>
<td>The OID tree that this entry will include or exclude.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates if this entry includes or excludes the OID tree.</td>
</tr>
</tbody>
</table>

2.9.31 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Flag</td>
<td>Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.</td>
</tr>
<tr>
<td>Link Up/Down Flag</td>
<td>Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.</td>
</tr>
<tr>
<td>Multiple Users Flag</td>
<td>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).</td>
</tr>
<tr>
<td>Spanning Tree Flag</td>
<td>Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.</td>
</tr>
<tr>
<td>ACL Traps</td>
<td>May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.</td>
</tr>
<tr>
<td>DVMRP Traps</td>
<td>Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.</td>
</tr>
<tr>
<td>OSPFv2 Traps</td>
<td>Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays disabled. Otherwise, the command shows all the enabled OSPF traps' information.</td>
</tr>
<tr>
<td>OSPFv3 Traps</td>
<td>Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPFv3 trap flags are not enabled, then the command displays disabled. Otherwise, the command shows all the enabled OSPFv3 traps' information.</td>
</tr>
<tr>
<td>PIM Traps</td>
<td>Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.</td>
</tr>
</tbody>
</table>
2.10 RADIUS Commands

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

2.10.1 aaa server radius dynamic-author

This command enables CoA functionality and enters dynamic authorization local server configuration mode.

Default: None
Format: aaa server radius dynamic-author
Mode: Global Config

Example:
(FASTPATH Routing) #configure
(FASTPATH Routing) (Config)#aaa server radius dynamic-author
(FASTPATH Routing) (Config- radius-da)#

2.10.1.1 no aaa server radius dynamic-author

This command disables CoA functionality.

Default: None
Format: no aaa server radius dynamic-author
Mode: Global Config

Example:
(FASTPATH Routing) #configure
(FASTPATH Routing) (Config)#no aaa server radius dynamic-author

2.10.2 authentication command bounce-port ignore

This command configures the device to ignore a RADIUS server bounce-host-port command. The bounce-host-port command causes a host to flap the link on an authentication port. The link flap causes DHCP renegotiation from one or more hosts connected to this port.

Default: FALSE (Bounce-Port messages will be processed)
Format: authentication command bounce-port ignore
Mode: Global Config

Example:
(Route) #configure
(Route) (Config)#authentication command bounce-port ignore
2.10.2.1  no authentication command bounce-port ignore

This command resets the device to the default value so that RADIUS server bounce-host-port commands are processed.

**Format**

```
no authentication command bounce-port ignore
```

**Mode**

Global Config

**Example:**

(Routing) #configure
(Routing) (Config)#no authentication command bounce-port ignore

2.10.3  auth-type

Use this command to specify the type of authorization that the device uses for RADIUS clients. The client must match the configured attributes for authorization.

**Default**

All

**Format**

```
auth-type { any | all | session-key }
```

**Mode**

Dynamic Authorization

**Example:**

(FASTPATH Routing) (Config- radius-da)#auth-type all

2.10.3.1  no auth-type

Use this command to reset the type of authorization that the device must use for RADIUS clients.

**Default**

None

**Format**

```
no auth-type
```

**Mode**

Dynamic Authorization

**Example:**

(FASTPATH Routing) (Config- radius-da)#no auth-type

2.10.4  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

2.10.4.1  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
2.10.5 clear radius dynamic-author statistics
This command clears radius dynamic authorization counters.

Default None
Format clear radius dynamic-author statistics
Mode Privileged EXEC

Example:
(FASTPATH Routing) #clear radius dynamic-author statistics
Are you sure you want to clear statistics? (y/n) y
Statistics cleared.

2.10.6 client
Use this command to configure the IP address or hostname of the AAA server client. Use the optional server-key keyword and string argument to configure the server key at the client level.

Default None
Format client { ip-address | hostname } [server-key [0|7] key-string]
Mode Dynamic Authorization

Example:
(FASTPATH Routing) (Config-radius-da)#client 10.0.0.1 server-key 7 device1

2.10.6.1 no client
Use this command to remove the configured Dynamic Authorization client and the key associated with that client in the device.

Default None
Format no client { ip-address | hostname }
Mode Dynamic Authorization

Example:
(FASTPATH Routing) (Config-radius-da)#no client 10.0.0.1

2.10.7 debug aaa coa
Use this command to display Dynamic Authorization Server processing debug information.

Default None
Format debug aaa coa
Mode Dynamic Authorization
2.10.8  debug aaa pod
Use this command to display Disconnect Message packets.

Default: None
Format: debug aaa pod
Mode: Dynamic Authorization

2.10.9  ignore server-key
Use this optional command to configure the device to ignore the server key.

Default: Disable
Format: ignore server-key
Mode: Dynamic Authorization

Example:
(FASTPATH Routing) (Config- radius-da)#ignore server-key

2.10.9.1 no ignore server-key
Use this optional command to configure the device not to ignore the server key (that is, it resets the ignore server key property on the device).

Default: Disable
Format: no ignore server-key
Mode: Dynamic Authorization

Example:
(FASTPATH Routing) (Config- radius-da)#no ignore server-key

2.10.10 ignore session-key
Use this optional command to configure the device to ignore the session key.

Default: Disable
Format: ignore session-key
Mode: Dynamic Authorization

Example:
(FASTPATH Routing) (Config- radius-da)#ignore session-key
2.10.10.1 no ignore session-key

Use this optional command to configure the device to not ignore the session key (that is, it resets the ignore session key property on the device).

**Default**: Disable

**Format**: `no ignore session-key`

**Mode**: Dynamic Authorization

**Example**:

(FASTPATH Routing) (Config-radius-da)#no ignore session-key

2.10.11 port

Use this command to specify the UDP port on which a device listens for RADIUS requests from configured Dynamic Authorization clients. The supported range for the port-number is 1025 to 65535.

**Default**: 3799

**Format**: `port port-number`

**Mode**: Dynamic Authorization

**Example**:

(FASTPATH Routing) (Config-radius-da)#port 1700

2.10.11.1 no port

Use this command to reset the configured UDP port on which a device listens for RADIUS requests from configured Dynamic Authorization clients.

**Default**: 3799

**Format**: `no port`

**Mode**: Dynamic Authorization

**Example**:

(FASTPATH Routing) (Config-radius-da)#no port

2.10.12 radius accounting mode

This command is used to enable the RADIUS accounting function.

**Default**: disabled

**Format**: `radius accounting mode`

**Mode**: Global Config
2.10.12.1 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

2.10.13 radius server attribute

This command specifies the RADIUS client to use the specified RADIUS attribute in the RADIUS requests. The supported attributes are as follows:

- **4**: Include the NAS-IP Address attribute. 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.
- **95**: Include the NAS-IPV6-Address attribute. If the specific IPv6 address is configured while enabling this attribute, the RADIUS client uses that IPv6 address while sending NAS-IPV6-Address attribute in RADIUS communication.
- **31**: This command configures the format in which the MAC address is sent to the RADIUS server. Use the `ipaddr` option to specify the RADIUS server to which the MAC address format is applicable. If no IP address is provided, the format applies to all RADIUS servers.

**Default**

(Attribute 31 only) MAC address format: legacy lower case

**Format**

radius server attribute {4 [ipaddr] | 95 [ipv6_addr] | 31 mac-format {legacy lower-case | upper-case | ietf lower-case | upper-case | unformatted lower-case | upper-case } [ipaddr]}

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>NAS-IP-Address attribute to be used in RADIUS requests.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>ipv6_addr</td>
<td>The IPv6 address of the server.</td>
</tr>
<tr>
<td>unformatted</td>
<td>Format the MAC address as aaaaabbbbcccc.</td>
</tr>
</tbody>
</table>

**Example:** The following shows an example of the command.

(Switch) (Config) #radius server attribute 4  192.168.37.60

**Example:** The following shows an example of the command.

(Switch) (Config) #(Config)#radius server attribute 95 3ffe:ffff:100:f101::1

**Example:** The following shows an example of the command.

(Switch) (Config) #(Config)#radius server attribute 31 mac-format unformatted lower-case
2.10.13.1 no radius server attribute

The no version of this command resets the RADIUS attributes to their default values. For attributes 4 and 95, this command disables the specified attribute global parameter for the RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address or NAS-IPV6-Address attribute in RADIUS requests.

Format: `no radius server attribute {4 [ipaddr] | 95 [ipv6_addr] | 31 mac-format}`
Mode: Global Config

2.10.14 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.

To reconfigure 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.

To reconfigure 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>dnsname</td>
<td>The DNS name of the server.</td>
</tr>
<tr>
<td>0-65535</td>
<td>The port number to use to connect to the specified RADIUS server.</td>
</tr>
<tr>
<td>servername</td>
<td>The alias name to identify the server.</td>
</tr>
</tbody>
</table>
2.10.14.1 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_RS port 1813
(Switch) (Config) #radius server host acct 192.168.37.60 name Network2_RS
(Switch) (Config) #no radius server host acct 192.168.37.60

2.10.15 radius server host link-local

This command configures the link-local-address of the RADIUS server and the outgoing interface to be used by the RADIUS client to communicate with the RADIUS server. The outgoing interface can be any physical interface or service port or network port.

Default  
None

Format  
radius server host {auth | acct} link-local link-local-address interface {unit/slot/port | network | serviceport} [name servername] [port port]

Mode  
Global Config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-local-address</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>interface</td>
<td>The interface for the RADIUS client to use for outgoing RADIUS messages.</td>
</tr>
<tr>
<td>servername</td>
<td>The alias name to identify the server.</td>
</tr>
<tr>
<td>port</td>
<td>The port number to use to connect to the specified RADIUS server.</td>
</tr>
</tbody>
</table>

Example: The following shows examples of the command.

(Switch) (Config) #radius server host auth link-local fe80::208:a1ff:fe7e:4519 interface network name auth_server port 1813

(Switch) (Config) #radius server host acct link-local fe80::208:a1ff:fe7e:4519 interface serviceport name acct_server port 1813
2.10.15.1  no radius server host link-local
This command removes the configured radius server link-local-address.

Default     None
Format       radius server host {auth | acct} link-local link-local-address
Mode        Global Config

Example: The following shows an example of the command.
(Switch) (Config) #no radius server host auth link-local fe80::208:a1ff:fe7e:4519

2.10.16   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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>dnsname</td>
<td>The DNS name of the server.</td>
</tr>
<tr>
<td>password</td>
<td>The password in encrypted format.</td>
</tr>
</tbody>
</table>

Example: The following shows an example of the CLI command.
radius server key acct 10.240.4.10 encrypted encrypt-string

2.10.17   radius server msgauth
This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip addr</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>dnsname</td>
<td>The DNS name of the server.</td>
</tr>
</tbody>
</table>

Date: 9 March 2019

wv14621 2019-03-09
### 2.10.17.1 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

### 2.10.18 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip addr</td>
<td>The IP address of the RADIUS Authenticating server.</td>
</tr>
<tr>
<td>dnsname</td>
<td>The DNS name of the server.</td>
</tr>
</tbody>
</table>

### 2.10.19 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retries</td>
<td>The maximum number of transmission attempts in the range of 1 to 15.</td>
</tr>
</tbody>
</table>

### 2.10.19.1 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
2.10.20  radius source-interface

Use this command to specify the physical or logical interface to use as the RADIUS client source interface (Source IP address). If configured, the address of source Interface is used for all RADIUS communications between the RADIUS server and the RADIUS client. The selected source-interface IP address is used for filling the IP header of RADIUS management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the RADIUS client falls back to its default behavior.

Format  radius source-interface {slot/port | loopback loopback-id | vlan vlan-id}
Mode    Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>The unit identifier assigned to the switch.</td>
</tr>
<tr>
<td>loopback-id</td>
<td>Configures the loopback interface. The range of the loopback ID is 0 to 7.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.</td>
</tr>
</tbody>
</table>

2.10.20.1  no radius source-interface

Use this command to reset the RADIUS source interface to the default settings.

Format  no radius source-interface
Mode    Global Config

2.10.21  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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retries</td>
<td>Maximum number of transmission attempts in the range 1–30.</td>
</tr>
</tbody>
</table>
2.10.21 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

2.10.22 server-key
Use this command to configure a global shared secret that is used for all dynamic authorization clients that do not have an individual shared secret key configured.

**Default**
None

**Format**
server-key [7] key-string

**Mode**
Dynamic Authorization

### Example:
(FASTPATH Routing) (Config-radius-da)# server-key encrypted mydevice

2.10.22.1 no server-key
Use this command to remove the global shared secret key configuration.

**Default**
None

**Format**
no server-key

**Mode**
Dynamic Authorization

### Example:
(FASTPATH Routing) (Config-radius-da)#no server-key

2.10.23 show radius servers
This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

**Format**
show radius servers \{ipaddr | ipv6addr | dnsname | name \[servername\]\}

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\ipaddr</td>
<td>The IP address of the authenticating server.</td>
</tr>
<tr>
<td>\ipv6addr</td>
<td>The IPv6 address of the server.</td>
</tr>
<tr>
<td>\dnsname</td>
<td>The DNS name of the authenticating server.</td>
</tr>
<tr>
<td>\servername</td>
<td>The alias name to identify the server.</td>
</tr>
</tbody>
</table>
### Command Output Fields

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>The * symbol preceding the server host address specifies that the server is currently active.</td>
</tr>
<tr>
<td>Host Address</td>
<td>The IP address of the host.</td>
</tr>
<tr>
<td>Server Name</td>
<td>The name of the authenticating server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used for communication with the authenticating server.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether this server is a primary or secondary type.</td>
</tr>
<tr>
<td>Current Host Address (*)</td>
<td>An asterisk (*) indicates which configured RADIUS host is the currently active authenticating server.</td>
</tr>
<tr>
<td>Number of Retransmits</td>
<td>The configured value of the maximum number of times a request packet is retransmitted.</td>
</tr>
<tr>
<td>Timeout Duration</td>
<td>The configured timeout value, in seconds, for request retransmissions.</td>
</tr>
<tr>
<td>RADIUS Accounting Mode</td>
<td>A global parameter to indicate whether the accounting mode for all the servers is enabled or not.</td>
</tr>
<tr>
<td>RADIUS Attribute 4 Mode</td>
<td>A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.</td>
</tr>
<tr>
<td>RADIUS Attribute 4 Value</td>
<td>A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.</td>
</tr>
<tr>
<td>RADIUS Attribute 95 Mode</td>
<td>A global parameter to indicate whether the NAS-IPv6-Address attribute has been enabled to use in RADIUS requests.</td>
</tr>
<tr>
<td>RADIUS Attribute 95 Value</td>
<td>A global parameter that specifies the IPv6 address to be used in NAS-IPv6-Address attribute to be used in RADIUS requests.</td>
</tr>
<tr>
<td>Link local interface</td>
<td>If configured, the link local IPv6 address.</td>
</tr>
<tr>
<td>Secret Configured</td>
<td>Yes or No Boolean value that indicates whether this server is configured with a secret.</td>
</tr>
<tr>
<td>Message Authenticator</td>
<td>A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.</td>
</tr>
<tr>
<td>CoA Bounce-Host-Port</td>
<td>Indicates whether RADIUS server Bounce-Port messages will be processed (Accept) or ignored.</td>
</tr>
<tr>
<td>Number of CoA Requests Received</td>
<td>The number of RADIUS Change of Authorization (CoA) requests messages received from a RADIUS host.</td>
</tr>
<tr>
<td>Number of CoA ACK Responses Sent</td>
<td>The number of RADIUS CoA acknowledgments the client has sent.</td>
</tr>
<tr>
<td>Number of CoA NAK Responses Sent</td>
<td>The number of RADIUS CoA non-acknowledgments the client has sent.</td>
</tr>
<tr>
<td>Number of CoA Requests Ignored</td>
<td>The number of RADIUS CoA requests the client has ignored.</td>
</tr>
<tr>
<td>Number of CoA Missing/ Unsupported Attribute R</td>
<td>The number of RADIUS CoA requests the client has received that have a missing or unsupported attribute value.</td>
</tr>
<tr>
<td>Number of CoA Session Context Not Found Request</td>
<td>The number of RADIUS CoA requests the client has received in which the session context identified in the CoA-Request or not exist on the NAS.</td>
</tr>
<tr>
<td>Number of CoA Invalid Attribute Value Request</td>
<td>The number of RADIUS CoA requests the client has received that have an invalid attribute value.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(Switch)  #show radius servers

<table>
<thead>
<tr>
<th>Current</th>
<th>Host Address</th>
<th>Server Name</th>
<th>Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>192.168.37.200</td>
<td>Network1_RADIUS_Server</td>
<td>1813</td>
<td>Primary</td>
</tr>
<tr>
<td></td>
<td>192.168.37.201</td>
<td>Network2_RADIUS_Server</td>
<td>1813</td>
<td>Secondary</td>
</tr>
<tr>
<td></td>
<td>192.168.37.202</td>
<td>Network3_RADIUS_Server</td>
<td>1813</td>
<td>Primary</td>
</tr>
<tr>
<td></td>
<td>192.168.37.203</td>
<td>Network4_RADIUS_Server</td>
<td>1813</td>
<td>Secondary</td>
</tr>
</tbody>
</table>

(Switch)  #show radius servers name

<table>
<thead>
<tr>
<th>Current Host Address</th>
<th>Server Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.37.200</td>
<td>Network1_RADIUS_Server</td>
<td></td>
</tr>
<tr>
<td>192.168.37.201</td>
<td>Network2_RADIUS_Server</td>
<td>Secondary</td>
</tr>
<tr>
<td>192.168.37.202</td>
<td>Network3_RADIUS_Server</td>
<td>Secondary</td>
</tr>
<tr>
<td>192.168.37.203</td>
<td>Network4_RADIUS_Server</td>
<td>Primary</td>
</tr>
</tbody>
</table>

(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
RADIUS Attribute 95 Mode............ Enable
RADIUS Attribute 95 Value........... 45:45::9

(Switch)  #show radius servers 192.168.2.10

RADIUS Server IP Address............... 192.168.2.10
RADIUS Server Name..................... Default-RADIUS-Server
Number of Retransmits.................. 4
Timeout Duration....................... 5
RADIUS Accounting Mode................ Disable
RADIUS Attribute 4 Mode.............. Disable
RADIUS Attribute 4 Value............. 0.0.0.0
RADIUS Attribute 95 Mode............. Disable
RADIUS Attribute 95 Value........... ::
Link local interface.................. Not Available
Port.................................. 1812
Type.................................. Secondary
Secret Configured...................... No
Message Authenticator.................. Enable
CoA Bounce-Host-Port................... Accept
Number of CoA Requests Received........ 0
Number of CoA ACK Responses Sent....... 0
Number of CoA NAK Responses Sent........ 0
Number of CoA Requests Ignored.......... 0
Number of CoA Missing/Unsupported Attribute R........ 0
Number of CoA Session Context Not Found Requests........ 0
Number of CoA Invalid Attribute Value Requests........ 0
Number of Administratively Prohibited Requests........ 0
2.10.24 show radius

This command displays the values configured for the global parameters of the RADIUS client.

**Format**
```
show radius
```

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Configured Authentication Servers</td>
<td>The number of RADIUS Authentication servers that have been configured.</td>
</tr>
<tr>
<td>Number of Configured Accounting Servers</td>
<td>The number of RADIUS Accounting servers that have been configured.</td>
</tr>
<tr>
<td>Number of Named Authentication Server Groups</td>
<td>The number of configured named RADIUS server groups.</td>
</tr>
<tr>
<td>Number of Named Accounting Server Groups</td>
<td>The number of configured named RADIUS server groups.</td>
</tr>
<tr>
<td>Number of Retransmits</td>
<td>The configured value of the maximum number of times a request packet is retransmitted.</td>
</tr>
<tr>
<td>Time Duration</td>
<td>The configured timeout value, in seconds, for request retransmissions.</td>
</tr>
<tr>
<td>RADIUS Accounting Mode</td>
<td>A global parameter to indicate whether the accounting mode for all the servers is enabled or not.</td>
</tr>
<tr>
<td>RADIUS Attribute 4 Mode</td>
<td>A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.</td>
</tr>
<tr>
<td>RADIUS Attribute 4 Value</td>
<td>A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.</td>
</tr>
</tbody>
</table>

**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
```

2.10.25 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>The IP address of the authenticating server.</td>
</tr>
<tr>
<td>dnsname</td>
<td>The DNS name of the authenticating server.</td>
</tr>
<tr>
<td>servername</td>
<td>The alias name to identify the server.</td>
</tr>
<tr>
<td>Current</td>
<td>The * symbol preceding the server host address specifies that the server is currently active.</td>
</tr>
<tr>
<td>Host Address</td>
<td>The IP address of the host.</td>
</tr>
<tr>
<td>Server Name</td>
<td>The name of the authenticating server.</td>
</tr>
</tbody>
</table>
The following shows example CLI display output for the command.

```
(Switch) #show radius servers

<table>
<thead>
<tr>
<th>Current Host Address</th>
<th>Server Name</th>
<th>Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 192.168.37.200</td>
<td>Network1_RADIUS_Server</td>
<td>1813</td>
<td>Primary</td>
</tr>
<tr>
<td>192.168.37.201</td>
<td>Network2_RADIUS_Server</td>
<td>1813</td>
<td>Secondary</td>
</tr>
<tr>
<td>192.168.37.202</td>
<td>Network3_RADIUS_Server</td>
<td>1813</td>
<td>Primary</td>
</tr>
<tr>
<td>192.168.37.203</td>
<td>Network4_RADIUS_Server</td>
<td>1813</td>
<td>Secondary</td>
</tr>
</tbody>
</table>

(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
```

**Field** | **Description**
---|---
Port | The port used for communication with the authenticating server.
Type | Specifies whether this server is a primary or secondary type.
Current Host Address | The IP address of the currently active authenticating server.
Secret Configured | Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits | The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator | A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration | The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode | A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode | A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value | A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.
2.10.26  show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format
show radius accounting name [servername]

Mode
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>servername</td>
<td>An alias name to identify the server.</td>
</tr>
<tr>
<td>RADIUS Accounting</td>
<td>A global parameter to indicate whether the accounting mode for all the servers is enabled or not.</td>
</tr>
</tbody>
</table>

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

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

(Switch) #show radius accounting name

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Server Name</th>
<th>Port</th>
<th>Secret Configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.37.200</td>
<td>Network1_RADIUS_Server</td>
<td>1813</td>
<td>Yes</td>
</tr>
<tr>
<td>192.168.37.201</td>
<td>Network2_RADIUS_Server</td>
<td>1813</td>
<td>No</td>
</tr>
<tr>
<td>192.168.37.202</td>
<td>Network3_RADIUS_Server</td>
<td>1813</td>
<td>Yes</td>
</tr>
<tr>
<td>192.168.37.203</td>
<td>Network4_RADIUS_Server</td>
<td>1813</td>
<td>No</td>
</tr>
</tbody>
</table>

(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
2.10.27 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>dnsname</td>
<td>The DNS name of the server.</td>
</tr>
<tr>
<td>servername</td>
<td>The alias name to identify the server.</td>
</tr>
<tr>
<td>RADIUS Accounting Server Name</td>
<td>The name of the accounting server.</td>
</tr>
<tr>
<td>Server Host Address</td>
<td>The IP address of the host.</td>
</tr>
<tr>
<td>Round Trip Time</td>
<td>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.</td>
</tr>
<tr>
<td>Requests</td>
<td>The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.</td>
</tr>
<tr>
<td>Retransmission</td>
<td>The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.</td>
</tr>
<tr>
<td>Responses</td>
<td>The number of RADIUS packets received on the accounting port from this server.</td>
</tr>
<tr>
<td>Malformed Responses</td>
<td>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.</td>
</tr>
<tr>
<td>Bad Authenticators</td>
<td>The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>The number of accounting timeouts to this server.</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>The number of RADIUS packets of unknown types, which were received from this server on the accounting port.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.</td>
</tr>
</tbody>
</table>

**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............................... 0.000
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

2.10.28 show radius source-interface
Use this command in Privileged EXEC mode to display the configured RADIUS client source-interface (Source IP address) information.

Format show radius source-interface
Mode Privileged EXEC

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

(Routing)# show radius source-interface
RADIUS Client Source Interface............. (not configured)

2.10.29 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>dnsname</td>
<td>The DNS name of the server.</td>
</tr>
<tr>
<td>servername</td>
<td>The alias name to identify the server.</td>
</tr>
<tr>
<td>RADIUS Server Name</td>
<td>The name of the authenticating server.</td>
</tr>
<tr>
<td>Server Host Address</td>
<td>The IP address of the host.</td>
</tr>
<tr>
<td>Access Requests</td>
<td>The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.</td>
</tr>
<tr>
<td>Access Retransmissions</td>
<td>The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.</td>
</tr>
<tr>
<td>Access Accepts</td>
<td>The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Access Rejects</td>
<td>The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Access Challenges</td>
<td>The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Malformed Access Responses</td>
<td>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.</td>
</tr>
<tr>
<td>Bad Authenticators</td>
<td>The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

```text
(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
```

```text
(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
```

### 2.11 TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

#### 2.11.1 tacacs-server host

Use the **tacacs-server host** command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. Use the **ip-address**, **ipv6-address**, or **hostname** parameter to specify the IPv4 address, IPv6 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 | ipv6-address | hostname} |
|----------------|--------------------------------|
| Mode           | Global Config                  |

**Pending Requests**
The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.

**Timeouts**
The number of authentication timeouts to this server.

**Unknown Types**
The number of packets of unknown type that were received from this server on the authentication port.

**Packets Dropped**
The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.
2.11.1 no tacacs-server host
Use the `no tacacs-server host` command to delete the specified hostname or IP address. The `ip-address`, `ipv6-address`, or `hostname` parameter is the IPv4 address, IPv6 address, or hostname of the TACACS+ server.

**Format**
```
no tacacs-server host {ip-address | ipv6-address | hostname}
```

**Mode**
Global Config

2.11.2 tacacs-server host link-local
Use this command to configure the link-local-address of the TACACS+ server and the outgoing interface to be used by the TACACS+ client to communicate with the TACACS+ server. The outgoing interface can be any physical interface, the service port, or the network port.

**Format**
```
tacacs-server host link-local link-local-address interface {unit/slot/port | network | serviceport}
```

**Mode**
Global Config

2.11.2.1 no tacacs-server host link-local
Use this command to remove the configured TACACS+ server link-local address.

**Format**
```
no tacacs-server host link-local
```

**Mode**
Global Config

2.11.3 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
2.11.3.1 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

2.11.4 tacacs-server keystring

Use the tacacs-server keystring command to set the global authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

**Format**

```
tacacs-server keystring
```

**Mode**

Global Config

**Example:** The following shows an example of the CLI command.

(Switching)(Config)#tacacs-server keystring
Enter tacacs key:********
Re-enter tacacs key:********

2.11.5 tacacs-server source-interface

Use this command in Global Configuration mode to configure the source interface (Source IP address) for TACACS+ server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

**Format**

```
tacacs-server source-interface {slot/port|loopback loopback-id|vlan vlan-id}
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>The unit identifier assigned to the switch, in slot/port format.</td>
</tr>
<tr>
<td>loopback-id</td>
<td>The loopback interface. The range of the loopback ID is 0 to 7.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.</td>
</tr>
</tbody>
</table>

**Example:** The following shows an example of the command.

```
(Config)#tacacs-server source-interface loopback 0
(Config)#tacacs-server source-interface 0/1
(Config)#no tacacs-server source-interface
```
2.11.5.1 no tacacs-server source-interface

Use this command in Global Configuration mode to remove the global source interface (Source IP selection) for all TACACS+ communications between the TACACS+ client and the server.

Format  no tacacs-server source-interface
Mode     Global Config

2.11.6 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. If you do not specify a timeout value, the command sets the global timeout to the default value. TACACS+ servers that do not use the global timeout will retain their configured timeout values.

Default  5
Format    tacacs-server timeout timeout
Mode      Global Config

2.11.6.1 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

2.11.7 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

2.11.8 keystring

Use the keystring command in TACACS Server Configuration mode to set the TACACS+ server-specific authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format  keystring
Mode     TACACS Server Config

Example: The following shows an example of the command.

(Switching)(Config)#tacacs-server host 1.1.1.1
(Switching)(Tacacs)#keystring

Enter tacacs key:********
Re-enter tacacs key:********
2.11.9 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

2.11.10 priority (TACACS Config)
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

2.11.11 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

2.11.12 show tacacs
Use the `show tacacs` command to display the configuration, statistics, and source interface details of the TACACS+ client.

Format: `show tacacs [ip-address | ipv6-address | hostname]`
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host address</td>
<td>The IP address or hostname of the configured TACACS+ server.</td>
</tr>
<tr>
<td>Port</td>
<td>The configured TACACS+ server port number.</td>
</tr>
<tr>
<td>TimeOut</td>
<td>The timeout in seconds for establishing a TCP connection.</td>
</tr>
<tr>
<td>Priority</td>
<td>The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.</td>
</tr>
</tbody>
</table>

**Example:** The following examples show output of this command.

(Broadcom FASTPATH Routing) #show tacacs
Global Timeout: 5

<table>
<thead>
<tr>
<th>Host address</th>
<th>Port</th>
<th>Timeout</th>
<th>Priority</th>
<th>Link Local Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.27.3.6</td>
<td>49</td>
<td>Global</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>200:25:dead:beaf::1</td>
<td>49</td>
<td>Global</td>
<td>0</td>
<td>Not Available</td>
</tr>
</tbody>
</table>
2.11.13  show tacacs source-interface

Use the `show tacacs source-interface` command in Global Config mode to display the configured global source interface details used for a TACACS+ client. The IP address of the selected interface is used as source IP for all communications with the server.

**Format**

```
show tacacs source-interface
```

**Mode**

Privileged EXEC

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

```
(Config)# show tacacs source-interface
TACACS Client Source Interface   : loopback 0
TACACS Client Source IPv4 Address : 1.1.1.1 [UP]
```

2.12  Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the `show running-config` command (see "show running-config" on page 134) to capture the running configuration into a script. Use the `copy` command (see "copy" on page 159) to transfer the configuration script to or from the switch.

Use the `show` command to view the configuration stored in the startup-config, backup-config, or factory-defaults file (see "show" on page 135).

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!
```

**NOTICE**

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
```

2.12.1 script apply
This command applies the commands in the script to the switch. The `scriptname` parameter is the name of the script to apply.

**Format**    
`script apply scriptname`

**Mode**        
Privileged EXEC

2.12.2 script delete
This command deletes a specified script where the `scriptname` parameter is the name of the script to delete. The `all` option deletes all the scripts present on the switch.

**Format**    
`script delete {scriptname | all}`

**Mode**        
Privileged EXEC

2.12.3 script list
This command lists all scripts present on the switch as well as the remaining available space.

**Format**    
`script list`

**Mode**        
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Script</td>
<td>Name of the script.</td>
</tr>
<tr>
<td>Size</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

2.12.4 script show
This command displays the contents of a script file, which is named `scriptname`.

**Format**    
`script show scriptname`

**Mode**        
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Format</td>
<td><code>line number: line contents</code></td>
</tr>
</tbody>
</table>

2.12.5 script validate
This command validates a script file by parsing each line in the script file where `scriptname` is the name of the script to validate. The `validate` option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

**Format**    
`script validate scriptname`

**Mode**        
Privileged EXEC
2.13 Prelogin Banner, System Prompt, and Host Name Commands

This section describes the commands you use to configure the prelogin banner and the system prompt. The prelogin banner is the text that displays before you login at the User: prompt.

2.13.1 copy (pre-login banner)

The copy command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using FTP, TFTP, SFTP, SCP, or Xmodem.

Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

---

**NOTICE**

The parameter *ip6address* is also a valid parameter for routing packages that support IPv6.

---

**Default**

none

**Format**

```plaintext
copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:clibanner

copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>
```

**Mode**

Privileged EXEC

2.13.2 set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

**Format**

```plaintext
set prompt prompt_string
```

**Mode**

Privileged EXEC

2.13.3 hostname

This command sets the system hostname. It also changes the prompt. The length of name may be up to 64 alphanumeric, case-sensitive characters.

**Format**

```plaintext
hostname hostname
```

**Mode**

Privileged EXEC

2.13.4 show clibanner

Use this command to display the configured prelogin CLI banner. The prelogin banner is the text that displays before displaying the CLI prompt.

**Default**

No contents to display before displaying the login prompt.

**Format**

```plaintext
show clibanner
```

**Mode**

Privileged EXEC

---

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

(Routing) #show clibanner

Banner Message configured :

```
========================================
|
---------
TEST
---------
```

---
2.13.5 set clibanner

Use this command to configure the prelogin CLI banner before displaying the login prompt.

**Format**

```
set clibanner line
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line</td>
<td>Banner text where &quot;&quot; (double quote) is a delimiting character. The banner message can be up to 2000 characters.</td>
</tr>
</tbody>
</table>

2.13.5.1 no set clibanner

Use this command to unconfigure the prelogin CLI banner.

**Format**

```
no set clibanner
```

**Mode**

Global Config
3/ Utility Commands

This chapter describes the utility commands available in the FASTPATH CLI. The Utility Commands chapter includes the following sections:

- “AutoInstall Commands” on page 114
- “CLI Output Filtering Commands” on page 116
- “Dual Image Commands” on page 118
- “System Information and Statistics Commands” on page 118
- “Logging Commands” on page 140
- “Email Alerting and Mail Server Commands” on page 147
- “System Utility and Clear Commands” on page 152
- “SFP handling Commands” on page 167
- “Commands to configure startup services” on page 169
- “Simple Network Time Protocol Commands” on page 169
- “Time Zone Commands” on page 174
- “DHCP Server Commands” on page 178
- “DNS Client Commands” on page 189
- “IP Address Conflict Commands” on page 194
- “Serviceability Packet Tracing Commands” on page 195
- “BCM Shell Command” on page 236
- “Cable Test Command” on page 237
- “sFlow Commands” on page 237
- “Switch Database Management Template Commands” on page 246
- “Remote Monitoring Commands” on page 249
- “Statistics Application Commands” on page 263
- “Precision Time Protocol (IEEE 1588) Commands” on page 268
- “Power Over Ethernet Commands” on page 281

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.
3.1 AutoInstall Commands

The AutoInstall feature enables the automatic update of the image and configuration of the switch. This feature enables touchless or low-touch provisioning to simplify switch configuration and imaging.

AutoInstall includes the following support:

- Downloading an image from TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.
- Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.
- Automatically downloading an image from a TFTP server in the following situations:
  - When the switch is booted with no saved configuration found.
  - When the switch is booted with a saved configuration that has AutoInstall enabled.

When the switch boots and no configuration file is found, it attempts to obtain an IP address from a network DHCP server. The response from the DHCP server includes the IP address of the TFTP server where the image and configuration files are located.

After acquiring an IP address and the additional relevant information from the DHCP server, the switch downloads the image file or configuration file from the TFTP server. A downloaded image is automatically installed. A downloaded configuration file is saved to non-volatile memory.

---

**NOTICE**

AutoInstall from a TFTP server can run on any IP interface, including the network port, service port, and in-band routing interfaces (if supported). To support AutoInstall, the DHCP client is enabled operationally on the service port, if it exists, or the network port, if there is no service port.

---

3.1.1 boot autoinstall

Use this command to operationally start or stop the AutoInstall process on the switch. The command is non-persistent and is not saved in the startup or running configuration file.

Default: stopped

Format: `boot autoinstall {start | stop}`

Mode: Privileged EXEC

3.1.2 boot host retrycount

Use this command to set the number of attempts to download a configuration file from the TFTP server.

Default: 3

Format: `boot host retrycount i-3`

Mode: Privileged EXEC

3.1.2.1 no boot host retrycount

Use this command to set the number of attempts to download a configuration file to the default value.

Format: `no boot host retrycount`

Mode: Privileged EXEC
3.1.3  boot host dhcp

Use this command to enable AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM.

Default: enabled
Format: boot host dhcp
Mode: Privileged EXEC

3.1.3.1  no boot host dhcp

Use this command to disable AutoInstall for the next reboot cycle.

Format: no boot host dhcp
Mode: Privileged EXEC

3.1.4  boot host autosave

Use this command to automatically save the downloaded configuration file to the startup-config file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to non-volatile memory by using the write memory or copy system:running-config nvram:startup-config command. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.

Default: enabled
Format: boot host autosave
Mode: Privileged EXEC

3.1.4.1  no boot host autosave

Use this command to disable automatically saving the downloaded configuration on the switch.

Format: no boot host autosave
Mode: Privileged EXEC

3.1.5  boot host autoreboot

Use this command to allow the switch to automatically reboot after successfully downloading an image. When autoreboot is enabled, no administrative action is required to activate the image and reload the switch.

Default: enabled
Format: boot host autoreboot
Mode: Privileged EXEC
### 3.1.5.1 **no boot host autoreboot**

Use this command to prevent the switch from automatically rebooting after the image is downloaded by using the AutoInstall feature.

**Format**
```
no boot host autoreboot
```

**Mode**
Privileged EXEC

### 3.1.6 **erase startup-config**

Use this command to erase the text-based configuration file stored in non-volatile memory. If the switch boots and no startup-config file is found, the AutoInstall process automatically begins.

**Format**
```
erase startup-config
```

**Mode**
Privileged EXEC

### 3.1.7 **erase factory-defaults**

Use this command to erase the text-based factory-defaults file stored in non-volatile memory.

**Default**
Disable

**Format**
```
erase factory-defaults
```

**Mode**
Privileged EXEC

### 3.1.8 **show autoinstall**

This command displays the current status of the AutoInstall process.

**Format**
```
show autoinstall
```

**Mode**
Privileged EXEC

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

```
(switch) #show autoinstall

AutoInstall Mode............................ Stopped
AutoInstall Persistent Mode............... Disabled
AutoSave Mode............................. Disabled
AutoReboot Mode........................... Enabled
AutoInstall Retry Count.................... 3
```

### 3.2 CLI Output Filtering Commands

#### 3.2.1 **show xxx|include “string”**

The command `xxx` is executed and the output is filtered to only show lines containing the “string” match. All other non-matching lines in the output are suppressed.

**Example:** The following shows an example of the CLI command.

```
(Routing) #show running-config | include “spanning-tree”

spanning-tree configuration name "00-02-BC-42-F9-33"
spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w
```
3.2.2 show \texttt{xxx|include \textbf{"string" exclude \textbf{"string2"}}}

The command \texttt{xxx} is executed and the output is filtered to only show lines containing the \textbf{“string”} match and not containing the \textbf{“string2”} match. All other non-matching lines in the output are suppressed. If a line of output contains both the include and exclude strings then the line is not displayed.

\textit{Example:} The following shows example of the CLI command.
(Routing) \#show running-config | include “spanning-tree” exclude “configuration”

spanning-tree bpduguard
spanning-tree bpdufilter default
spanning-tree forceversion 802.1w

3.2.3 show \texttt{xxx|exclude \textbf{“string”}}

The command \texttt{xxx} is executed and the output is filtered to show all lines not containing the \textbf{“string”} match. Output lines containing the \textbf{“string”} match are suppressed.

\textit{Example:} The following shows an example of the CLI command.
(Routing) \#show interface 0/1

Packets Received Without Error.................. 0
Packets Received With Error.................... 0
Broadcast Packets Received...................... 0
Receive Packets Discarded...................... 0
Packets Transmitted Without Errors.............. 0
Transmit Packets Discarded...................... 0
Transmit Packet Errors........................... 0
Collision Frames.................................. 0
Time Since Counters Last Cleared................ 281 day 4 hr 9 min 0 sec

(Routing) \#show interface 0/1 | exclude “Packets”

Transmit Packet Errors........................... 0
Collision Frames.................................. 0
Time Since Counters Last Cleared................ 20 day 21 hr 30 min 9 sec

3.2.4 show \texttt{xxx|begin \textbf{“string”}}

The command \texttt{xxx} is executed and the output is filtered to show all lines beginning with and following the first line containing the \textbf{“string”} match. All prior lines are suppressed.

\textit{Example:} The following shows an example of the CLI command.
(Routing) \#show port all | begin “1/1”

1/1 Enable Down Disable N/A N/A
1/2 Enable Down Disable N/A N/A
1/3 Enable Down Disable N/A N/A
1/4 Enable Down Disable N/A N/A
1/5 Enable Down Disable N/A N/A
1/6 Enable Down Disable N/A N/A

(Routing) #

3.2.5 show \texttt{xxx|section \textbf{“string”}}

The command \texttt{xxx} is executed and the output is filtered to show only lines included within the section(s) identified by lines containing the \textbf{“string”} match and ending with the first line containing the default end-of-section identifier (i.e. “exit”).

\textit{Example:} The following shows an example of the CLI command.
(Routing) \#show running-config | section “interface 0/1”

interface 0/1
no spanning-tree port mode
exit
3.2.6  `show xxx|section “string” “string2”`

The command `xxx` is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the “string” match and ending with the first line containing the “string2” match. If multiple sessions matching the specified string match criteria are part of the base output, then all instances are displayed.

3.2.7  `show xxx|section “string” include “string2”`

The command `xxx` is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the “string” match and ending with the first line containing the default end-of-section identifier (i.e. “exit”) and that include the “string2” match. This type of filter command could also include “exclude” or user-defined end-of-section identifier parameters as well.

3.3  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.

3.3.1  `delete`

This command deletes the backup image file from the permanent storage or the core dump file from the local file system.

```
Format  delete backup
dele te core-dump-file file-name | all

Mode  Privileged EXEC
```

3.3.2  `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. If the specified image doesn’t exist on the system, this command returns an error message.

```
Format  boot system {active | backup}

Mode  Privileged EXEC
```

3.3.3  `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
```

3.4  System Information and Statistics Commands

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

3.4.1  `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
```
3.4.2 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

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

Event log information is retained across a switch reset.

3.4.3 show hardware

This command displays inventory information for the switch.

**Format**
```
show hardware
```

**Mode**
Privileged EXEC

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 "show version" on page 119.

3.4.4 show version

This command displays inventory information for the switch.

**Format**
```
show version
```

**Mode**
Privileged EXEC

The show version command will replace the show hardware command in future releases of the software.
3.4.5  show platform vpd

This command displays vital product data for the switch.

**Format**

`show platform vpd`

**Mode**

User Privileged

The following information is displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Code</td>
<td>Build Signature loaded into the switch.</td>
</tr>
<tr>
<td>Image File Name</td>
<td>Release Version Maintenance Level and Build (RVMB) information of the switch.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Timestamp at which the image is built</td>
</tr>
</tbody>
</table>

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

(Routing) #show platform vpd

Operational Code Image File Name.............. FastPath-Ent-esw-xgs4-gto-BL20R-CS-6AIQH5r3v7m14b35
Software Version........................................ 3.7.14.35
Timestamp............................................. Thu Mar  7 14:36:14 IST 2013

3.4.6  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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Received Without Error</td>
<td>The total number of packets (including broadcast packets and multicast packets) received by the processor.</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Received With Error</td>
<td>The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.</td>
</tr>
<tr>
<td>Receive Packets Discarded</td>
<td>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. One possible reason for discarding such a packet could be to free up buffered space.</td>
</tr>
<tr>
<td>Packets Transmitted Without Error</td>
<td>The total number of packets transmitted out of the interface.</td>
</tr>
<tr>
<td>Transmit Packets Discarded</td>
<td>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.</td>
</tr>
<tr>
<td>Transmit Packets Errors</td>
<td>The number of outbound packets that could not be transmitted because of errors.</td>
</tr>
<tr>
<td>Collisions Frames</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>Time Since Counters Last Cleared</td>
<td>The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.</td>
</tr>
</tbody>
</table>

The display parameters, when the argument is "switchport" are as follows:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Received Without Error</td>
<td>The total number of packets (including broadcast packets and multicast packets) received by the processor.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.</td>
</tr>
<tr>
<td>Packets Received With Error</td>
<td>The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</td>
</tr>
<tr>
<td>Packets Transmitted Without Error</td>
<td>The total number of packets transmitted out of the interface.</td>
</tr>
<tr>
<td>Broadcast Packets Transmitted</td>
<td>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.</td>
</tr>
<tr>
<td>Transmit Packet Errors</td>
<td>The number of outbound packets that could not be transmitted because of errors.</td>
</tr>
<tr>
<td>Time Since Counters Last Cleared</td>
<td>The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.</td>
</tr>
</tbody>
</table>

### 3.4.7 show interfaces status

Use this command to display interface information, including the description, port state, speed and auto-neg capabilities. The command is similar to `show port all` but displays additional fields like interface description and port-capability. The description of the interface is configurable through the existing command `description <name>` which has a maximum length of 64 characters that is truncated to 28 characters in the output. The long form of the description can be displayed using `show port description`. The interfaces displayed by this command are physical interfaces, LAG interfaces and VLAN routing interfaces.

**Format**

```
show interfaces status [<slot/port>]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The interface associated with the rest of the data in the row.</td>
</tr>
</tbody>
</table>
3.4.8 show interfaces traffic

Use this command to display interface traffic information.

**Format**
```
show interfaces traffic [slot/port]
```

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The descriptive user-configured name for the interface.</td>
</tr>
<tr>
<td>Link State</td>
<td>Indicates whether the link is up or down.</td>
</tr>
<tr>
<td>Physical Mode</td>
<td>The speed and duplex settings on the interface.</td>
</tr>
<tr>
<td>Physical Status</td>
<td>Indicates the port speed and duplex mode for physical interfaces. The physical status for LAGs is not reported. When a port is down, the physical status is unknown.</td>
</tr>
<tr>
<td>Media Type</td>
<td>The media type of the interface.</td>
</tr>
<tr>
<td>Flow Control Status</td>
<td>The 802.3x flow control status.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>The configured 802.3x flow control mode.</td>
</tr>
</tbody>
</table>

3.4.9 show interface counters

This command reports key summary statistics for all the ports (physical/CPU/port-channel).

**Format**
```
show interface counters
```

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The interface associated with the rest of the data in the row.</td>
</tr>
<tr>
<td>InOctects</td>
<td>The total number of octets received on the interface.</td>
</tr>
<tr>
<td>InUcastPkts</td>
<td>The total number of unicast packets received on the interface.</td>
</tr>
<tr>
<td>InMcastPkts</td>
<td>The total number of multicast packets received on the interface.</td>
</tr>
<tr>
<td>InBcastPkts</td>
<td>The total number of broadcast packets received on the interface.</td>
</tr>
<tr>
<td>OutOctects</td>
<td>The total number of octets transmitted by the interface.</td>
</tr>
<tr>
<td>OutUcastPkts</td>
<td>The total number of unicast packets transmitted by the interface.</td>
</tr>
<tr>
<td>OutMcastPkts</td>
<td>The total number of multicast packets transmitted by the interface.</td>
</tr>
<tr>
<td>OutBcastPkts</td>
<td>The total number of broadcast packets transmitted by the interface.</td>
</tr>
</tbody>
</table>

**Example:** The following shows example CLI display output for the command.
```
(Routing) # show interface counters
```
Port    | InOctets | InUcastPkts | InMcastPkts | InBcastPkts
---|---|---|---|---
0/1 | 0 | 0 | 0 | 0

Port    | InOctets | InUcastPkts | InMcastPkts | InBcastPkts
---|---|---|---|---
0/1 | 0 | 0 | 0 | 0
0/2 | 0 | 0 | 0 | 0
0/3 | 15098 | 0 | 31 | 39
0/4 | 0 | 0 | 0 | 0
0/5 | 0 | 0 | 0 | 0
... 
ch1 | 0 | 0 | 0 | 0
ch2 | 0 | 0 | 0 | 0
... 
ch64 | 0 | 0 | 0 | 0
CPU | 359533 | 0 | 3044 | 217

Port    | OutOctets | OutUcastPkts | OutMcastPkts | OutBcastPkts
---|---|---|---|---
0/1 | 0 | 0 | 0 | 0
0/2 | 0 | 0 | 0 | 0
0/3 | 131369 | 0 | 11 | 89
0/4 | 0 | 0 | 0 | 0
0/5 | 0 | 0 | 0 | 0
... 
ch1 | 0 | 0 | 0 | 0
ch2 | 0 | 0 | 0 | 0
... 
ch64 | 0 | 0 | 0 | 0
CPU | 4025293 | 0 | 32910 | 120

### 3.4.10 show interface ethernet

This command displays detailed statistics for a specific interface or for all CPU traffic based upon the argument.

**Format**

```plaintext
show interface ethernet {slot/port | switchport | all}
```

**Mode**

Privileged EXEC

When you specify a value for `slot/port`, the command displays the following information.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Packets Received** | Total Packets Received (Octets) - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.  
  • Packets Received 64 Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).  
  • Packets Received 65–127 Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).  
  • Packets Received 128–255 Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). |
<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Packets Received 256–511 Octets -</td>
<td>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).</td>
</tr>
<tr>
<td>• Packets Received 512–1023 Octets -</td>
<td>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).</td>
</tr>
<tr>
<td>• Packets Received 1024–1518 Octets -</td>
<td>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).</td>
</tr>
<tr>
<td>• Packets Received &gt; 1518 Octets -</td>
<td>The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>• Packets RX and TX 64 Octets -</td>
<td>The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>• Packets RX and TX 65–127 Octets -</td>
<td>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).</td>
</tr>
<tr>
<td>• Packets RX and TX 128–255 Octets -</td>
<td>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).</td>
</tr>
<tr>
<td>• Packets RX and TX 256–511 Octets -</td>
<td>The total number of packets received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 512–1023 Octets -</td>
<td>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).</td>
</tr>
<tr>
<td>• Packets RX and TX 1024–1518 Octets -</td>
<td>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).</td>
</tr>
<tr>
<td>• Packets RX and TX 1519–2047 Octets -</td>
<td>The total number of packets received and transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>• Packets RX and TX 1523–2047 Octets -</td>
<td>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.</td>
</tr>
<tr>
<td>• Packets RX and TX 2048–4095 Octets -</td>
<td>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.</td>
</tr>
<tr>
<td>• Packets RX and TX 4096–9216 Octets -</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Packets Received Successfully</strong></td>
<td>• Total Packets Received Without Error - The total number of packets received that were without errors.</td>
</tr>
<tr>
<td>• Unicast Packets Received -</td>
<td>The number of subnetwork-unicast packets delivered to a higher-layer protocol.</td>
</tr>
<tr>
<td>• Multicast Packets Received -</td>
<td>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.</td>
</tr>
<tr>
<td>• Broadcast Packets Received -</td>
<td>The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.</td>
</tr>
<tr>
<td><strong>Receive Packets Discarded</strong></td>
<td>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. One possible reason for discarding such a packet could be to free up buffer space.</td>
</tr>
</tbody>
</table>
### Packets Received with MAC Errors

- **Total Packets Received with MAC Errors** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
- **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
- **Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
- **FCS Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.
- **Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
- **uRPF Discards** - The number of packets dropped due to failing the uRPF.

### Received Packets Not Forwarded

- **Total Received Packets Not Forwarded** - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process.
- **802.3x Pause Frames Received** - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
- **Unacceptable Frame Type** - The number of frames discarded from this port due to being an unacceptable frame type.

### Packets Transmitted Octets

- **Total Packets Transmitted (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
- **Packets Transmitted 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
- **Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Transmitted > 1518 Octets** - The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
- **Max Frame Size** - The maximum size of the Info (non-MAC) field that this port will receive or transmit.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Packets Transmitted Successfully** | • Total Packets Transmitted Successfully - The number of frames that have been transmitted by this port to its segment.  
• Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.  
• Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.  
• Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent. |
| **Transmit Packets Discarded** | The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space. |
| **Transmit Errors** | • Total Transmit Errors - The sum of Single, Multiple, and Excessive Collisions.  
• FCS Errors - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.  
• Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission. |
| **Transmit Discards** | • Total Transmit Packets Discards - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.  
• Single Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.  
• Multiple Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.  
• Excessive Collisions - A count of frames for which transmission on a particular interface fails due to excessive collisions.  
• Port Membership Discards - The number of frames discarded on egress for this port due to egress filtering being enabled. |
| **Protocol Statistics** | • 802.3x Pause Frames Transmitted - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.  
• GVRP PDUs Received - The count of GVRP PDUs received in the GARP layer.  
• GVRP PDUs Transmitted - The count of GVRP PDUs transmitted from the GARP layer.  
• GVRP Failed Registrations - The number of times attempted GVRP registrations could not be completed.  
• GMRP PDUs Received - The count of GMRP PDUs received in the GARP layer.  
• GMRP PDUs Transmitted - The count of GMRP PDUs transmitted from the GARP layer.  
• GMRP Failed Registrations - The number of times attempted GMRP registrations could not be completed.  
• STP BPDUs Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent.  
• STP BPDUs Received - Spanning Tree Protocol Bridge Protocol Data Units received.  
• RST BPDUs Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.  
• RSTP BPDUs Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received.  
• MSTP BPDUs Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.  
• MSTP BPDUs Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received. |
| **Dot1x Statistics** | • EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.  
• EAPOL Start Frames Received - The number of valid EAPOL start frames that have been received by this authenticator. |
| **Time Since Counters Last Cleared** | The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared. |
If you use the `switchport` keyword, the following information appears.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Received Without Error</td>
<td>The total number of packets (including broadcast packets and multicast packets) received by the processor.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.</td>
</tr>
<tr>
<td>Packets Received With Error</td>
<td>The total number of packets with errors (including broadcast packets and multicast packets) received by the processor.</td>
</tr>
<tr>
<td>Packets Transmitted without Errors</td>
<td>The total number of packets transmitted out of the interface.</td>
</tr>
<tr>
<td>Broadcast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>Transmit Packet Errors</td>
<td>The number of outbound packets that could not be transmitted because of errors.</td>
</tr>
<tr>
<td>Time Since Counters Last Cleared</td>
<td>The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.</td>
</tr>
</tbody>
</table>

If you use the `all` keyword, the following information appears for all interfaces on the switch.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The Interface ID.</td>
</tr>
<tr>
<td>Bytes Tx</td>
<td>The total number of bytes transmitted by the interface.</td>
</tr>
<tr>
<td>Bytes Rx</td>
<td>The total number of bytes transmitted by the interface.</td>
</tr>
<tr>
<td>Packets Tx</td>
<td>The total number of packets transmitted by the interface.</td>
</tr>
<tr>
<td>Packets Rx</td>
<td>The total number of packets transmitted by the interface.</td>
</tr>
</tbody>
</table>

### 3.4.11 show interface ethernet switchport

This command displays the private VLAN mapping information for the switch interfaces.

**Format**

`show interface ethernet interface-id switchport`

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-id</td>
<td>The slot/port of the switch.</td>
</tr>
</tbody>
</table>

The command displays the following information.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private-vlan host-association</td>
<td>The VLAN association for the private-VLAN host ports.</td>
</tr>
<tr>
<td>Private-vlan mapping</td>
<td>The VLAN mapping for the private-VLAN promiscuous ports.</td>
</tr>
</tbody>
</table>

### 3.4.12 show interface lag

Use this command to display configuration information about the specified LAG interface.

**Format**

`show interface lag Lag-intf-num`

**Mode**

Privileged EXEC
3.4.13 show fiber-ports optical-transceiver

This command displays the diagnostics information of the SFP like Temp, Voltage, Current, Input Power, Output Power, Tx Fault, and LOS. The values are derived from the SFP’s A2 (Diagnostics) table using the I2C interface.

**Format**

```
show fiber-ports optical-transceiver {all | slot/port}
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>Internally measured transceiver temperature.</td>
</tr>
<tr>
<td>Voltage</td>
<td>Internally measured supply voltage.</td>
</tr>
<tr>
<td>Current</td>
<td>Measured TX bias current.</td>
</tr>
<tr>
<td>Output Power</td>
<td>Measured optical output power relative to 1mW.</td>
</tr>
<tr>
<td>Input Power</td>
<td>Measured optical power received relative to 1mW.</td>
</tr>
<tr>
<td>TX Fault</td>
<td>Transmitter fault.</td>
</tr>
<tr>
<td>LOS</td>
<td>Loss of signal.</td>
</tr>
</tbody>
</table>

**Example:** The following information shows an example of the command output:

(Switch) #show fiber-ports optical-transceiver all

<table>
<thead>
<tr>
<th>Port</th>
<th>Temp</th>
<th>Voltage</th>
<th>Current</th>
<th>Output Power</th>
<th>Input Power</th>
<th>TX Fault</th>
<th>LOS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[C]</td>
<td>[Volt]</td>
<td>[mA]</td>
<td>[dBm]</td>
<td>[dBm]</td>
<td>Fault</td>
<td></td>
</tr>
<tr>
<td>0/49</td>
<td>39.3</td>
<td>3.256</td>
<td>5.0</td>
<td>-2.234</td>
<td>-2.465</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0/50</td>
<td>33.9</td>
<td>3.260</td>
<td>5.3</td>
<td>-2.374</td>
<td>-40.000</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>0/51</td>
<td>32.2</td>
<td>3.256</td>
<td>5.6</td>
<td>-2.300</td>
<td>-2.897</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
3.4.14  show fiber-ports optical-transceiver-info

This command displays the SFP vendor related information like Vendor Name, Serial Number of the SFP, Part Number of the SFP. The values are derived from the SFP’s A0 table using the I2C interface.

**Format**  
show fiber-ports optical-transceiver-info {all | slot/port}

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Name</td>
<td>The vendor name is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h). The vendor name shall be the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.</td>
</tr>
<tr>
<td>Length (50um, OM2)</td>
<td>This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 50 micron multimode OM2 [500MHz·km at 850nm] fiber. A value of zero means that the transceiver does not support 50 micron multimode fiber or that the length information must be determined from the transceiver technology.</td>
</tr>
<tr>
<td>Length (62.5um, OM1)</td>
<td>This value specifies link length that is supported by the transceiver while operating in compliance with applicable standards using 62.5 micron multimode OM1 [200 MHz·km at 850nm, 500 MHz·km at 1310nm] fiber. A value of zero means that the transceiver does not support 62.5 micron multimode fiber or that the length information must determined from the transceiver technology.</td>
</tr>
<tr>
<td>Vendor SN</td>
<td>The vendor serial number (vendor SN) is a 16 character field that contains ASCII characters, left-aligned and padded on the right with ASCII spaces (20h), defining the vendor’s serial number for the transceiver. A value of all zero in the 16-byte field indicates that the vendor SN is unspecified.</td>
</tr>
<tr>
<td>Vendor PN</td>
<td>The vendor part number (vendor PN) is a 16-byte field that contains ASCII characters, left aligned and added on the right with ASCII spaces (20h), defining the vendor part number or product name. A value of all zero in the 16-byte field indicates that the vendor PN is unspecified.</td>
</tr>
<tr>
<td>BR, nominal</td>
<td>The nominal bit (signaling) rate (BR, nominal) is specified in units of 100 MBd, rounded off to the nearest 100 MBd. The bit rate includes those bits necessary to encode and delimit the signal as well as those bits carrying data information. A value of 0 indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate will depend on the encoding of the data, as defined by the encoding value.</td>
</tr>
<tr>
<td>Vendor Rev</td>
<td>The vendor revision number (vendor rev) contains ASCII characters, left aligned and padded on the right with ASCII spaces (20h), defining the vendor’s product revision number. A value of all zero in this field indicates that the vendor revision is unspecified.</td>
</tr>
</tbody>
</table>

**Example:** The following information shows an example of the command output:

(Switch) #show fiber-ports optical-transceiver-info all

<table>
<thead>
<tr>
<th>Port</th>
<th>Vendor Name</th>
<th>Link Length 50um [m]</th>
<th>Link Length 62.5um [m]</th>
<th>Serial Number</th>
<th>Part Number</th>
<th>Nominal Rate [Mbps]</th>
<th>Rev</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/49</td>
<td>BROADCOM</td>
<td>8</td>
<td>3</td>
<td>A7N2018414</td>
<td>AXM761</td>
<td>10300</td>
<td>10</td>
</tr>
<tr>
<td>0/51</td>
<td>BROADCOM</td>
<td>8</td>
<td>3</td>
<td>A7N2018472</td>
<td>AXM761</td>
<td>10300</td>
<td>10</td>
</tr>
<tr>
<td>0/52</td>
<td>BROADCOM</td>
<td>8</td>
<td>3</td>
<td>A7N2018501</td>
<td>AXM761</td>
<td>10300</td>
<td>10</td>
</tr>
</tbody>
</table>
3.4.15  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.

Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number. 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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN in which the MAC address is learned.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.</td>
</tr>
<tr>
<td>Interface</td>
<td>The port through which this address was learned.</td>
</tr>
<tr>
<td>Interface Index</td>
<td>This object indicates the ifIndex of the interface table entry associated with this port.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of this entry. The meanings of the values are:</td>
</tr>
<tr>
<td></td>
<td>• Static—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned.</td>
</tr>
<tr>
<td></td>
<td>• Learned—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.</td>
</tr>
<tr>
<td></td>
<td>• Management—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing.</td>
</tr>
<tr>
<td></td>
<td>• Self—The value of the corresponding instance is the address of one of the switch”s physical interfaces (the system”s own MAC address).</td>
</tr>
<tr>
<td></td>
<td>• GMRP Learned—The value of the corresponding was learned via GMRP and applies to Multicast.</td>
</tr>
<tr>
<td></td>
<td>• Other—The value of the corresponding instance does not fall into one of the other categories.</td>
</tr>
</tbody>
</table>

If you enter vlan vlan_id, only the MAC Address, Interface, and Status fields appear. If you enter the interface slot/port parameter, in addition to the MAC Address and Status fields, the VLAN ID field also appears.

The following information displays if you enter the count parameter:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Address count</td>
<td>Number of MAC addresses in the forwarding database that were automatically learned.</td>
</tr>
<tr>
<td>Static Address (User-defined) count</td>
<td>Number of MAC addresses in the forwarding database that were manually entered by a user.</td>
</tr>
<tr>
<td>Total MAC Addresses in use</td>
<td>Number of MAC addresses currently in the forwarding database.</td>
</tr>
<tr>
<td>Total MAC Addresses available</td>
<td>Number of MAC addresses the forwarding database can handle.</td>
</tr>
</tbody>
</table>
3.4.16 process cpu threshold

Use this command to configure the CPU utilization thresholds. The Rising and Falling thresholds are specified as a percentage of CPU resources. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds. The CPU utilization threshold configuration is saved across a switch reboot. Configuring the falling utilization threshold is optional. If the falling CPU utilization parameters are not configured, then they take the same value as the rising CPU utilization parameters.

**Format**

```
process cpu threshold type total rising 1-100 interval
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rising threshold</td>
<td>The percentage of CPU resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).</td>
</tr>
<tr>
<td>rising interval</td>
<td>The duration of the CPU rising threshold violation, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).</td>
</tr>
<tr>
<td>falling threshold</td>
<td>The percentage of CPU resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled). A notification is triggered when the total CPU utilization falls below this level for a configured period of time. The falling utilization threshold notification is made only if a rising threshold notification was previously done. The falling utilization threshold must always be equal or less than the rising threshold value. The CLI does not allow setting the falling threshold to be greater than the rising threshold.</td>
</tr>
<tr>
<td>falling interval</td>
<td>The duration of the CPU falling threshold, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).</td>
</tr>
</tbody>
</table>

3.4.17 show process app-list

This command displays the user and system applications.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>PID</th>
<th>Admin Status</th>
<th>Auto Restart</th>
<th>Running Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dataplane</td>
<td>15309</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Running</td>
</tr>
<tr>
<td>2</td>
<td>switchdrvr</td>
<td>15310</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Running</td>
</tr>
<tr>
<td>3</td>
<td>syncdb</td>
<td>15314</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Running</td>
</tr>
<tr>
<td>4</td>
<td>lighttpd</td>
<td>18718</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Running</td>
</tr>
</tbody>
</table>

**NOTICE**

This command is available in Linux 2.6 only.

<table>
<thead>
<tr>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>show process app-list</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

**Example:** The following shows example CLI display output for the command.
3.4.18 show process app-resource-list

This command displays the configured and in-use resources of each application.

![Notice]

This command is available in Linux 2.6 only.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The application identifier.</td>
</tr>
<tr>
<td>Name</td>
<td>The name that identifies the process.</td>
</tr>
<tr>
<td>PID</td>
<td>The number the software uses to identify the process.</td>
</tr>
<tr>
<td>Memory Limit</td>
<td>The maximum amount of memory the process can consume.</td>
</tr>
<tr>
<td>CPU Share</td>
<td>The maximum percentage of CPU utilization the process can consume.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>The amount of memory the process is currently using.</td>
</tr>
<tr>
<td>Max Mem Usage</td>
<td>The maximum amount of memory the process has used at any given time since it started.</td>
</tr>
</tbody>
</table>

(Routing) #show process app-resource-list

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>PID</th>
<th>Memory Limit</th>
<th>CPU Share</th>
<th>Memory Usage</th>
<th>Max Mem Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>switchdrvrr</td>
<td>251</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>380 MB</td>
<td>381 MB</td>
</tr>
<tr>
<td>2</td>
<td>syncdb</td>
<td>252</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>0 MB</td>
<td>0 MB</td>
</tr>
<tr>
<td>3</td>
<td>syncdb-test</td>
<td>0</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>0 MB</td>
<td>0 MB</td>
</tr>
<tr>
<td>4</td>
<td>proctest</td>
<td>0</td>
<td>10 MB</td>
<td>20%</td>
<td>0 MB</td>
<td>0 MB</td>
</tr>
<tr>
<td>5</td>
<td>utelnetd</td>
<td>0</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>0 MB</td>
<td>0 MB</td>
</tr>
<tr>
<td>6</td>
<td>lxshTelnetd</td>
<td>0</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>0 MB</td>
<td>0 MB</td>
</tr>
<tr>
<td>7</td>
<td>user.start</td>
<td>0</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>0 MB</td>
<td>0 MB</td>
</tr>
</tbody>
</table>

3.4.19 show process cpu

This command provides the percentage utilization of the CPU by different tasks.

![Notice]

It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

![Notice]

This command is available in Linux 2.6 only.

| Format               | show process cpu [1-n | all] |
|----------------------|------------------------|
| Mode                 | Privileged EXEC        |
Example: The following shows example CLI display output for the command using Linux.

```
(Routing) #show process cpu
Memory Utilization Report
status        bytes
----------    -------
free  106450944
alloc 423227392

CPU Utilization:

<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>5 Secs</th>
<th>60 Secs</th>
<th>300 Secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>765</td>
<td>_interrupt_thread</td>
<td>0.00%</td>
<td>0.01%</td>
<td>0.02%</td>
</tr>
<tr>
<td>767</td>
<td>bcmL2X.0</td>
<td>0.58%</td>
<td>0.35%</td>
<td>0.28%</td>
</tr>
<tr>
<td>768</td>
<td>bcmCNTR.0</td>
<td>0.77%</td>
<td>0.73%</td>
<td>0.72%</td>
</tr>
<tr>
<td>773</td>
<td>bcmRX</td>
<td>0.00%</td>
<td>0.04%</td>
<td>0.05%</td>
</tr>
<tr>
<td>786</td>
<td>cpuUtilMonitorTask</td>
<td>0.19%</td>
<td>0.23%</td>
<td>0.23%</td>
</tr>
<tr>
<td>834</td>
<td>dotls_task</td>
<td>0.00%</td>
<td>0.01%</td>
<td>0.01%</td>
</tr>
<tr>
<td>818</td>
<td>hap1RxTask</td>
<td>0.00%</td>
<td>0.01%</td>
<td>0.01%</td>
</tr>
<tr>
<td>805</td>
<td>dtlTask</td>
<td>0.00%</td>
<td>0.02%</td>
<td>0.02%</td>
</tr>
<tr>
<td>863</td>
<td>spmTask</td>
<td>0.00%</td>
<td>0.01%</td>
<td>0.00%</td>
</tr>
<tr>
<td>894</td>
<td>ip6MapLocalDataTask</td>
<td>0.00%</td>
<td>0.01%</td>
<td>0.01%</td>
</tr>
<tr>
<td>908</td>
<td>RMONTask</td>
<td>0.00%</td>
<td>0.11%</td>
<td>0.12%</td>
</tr>
</tbody>
</table>

Total CPU Utilization 1.55% 1.58% 1.50%
```

3.4.20 show process proc-list

This application displays the processes started by applications created by the Process Manager.

**NOTICE**

This command is available in Linux 2.6 only.

**Format**

```
show process proc-list
```

**Mode**

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

(Routing) #show process proc-list

<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>Application</th>
<th>VM Size</th>
<th>VM Peak</th>
<th>FD Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>15260</td>
<td>procmgr</td>
<td>0-procmgr</td>
<td>No</td>
<td>1984</td>
<td>8</td>
</tr>
<tr>
<td>15309</td>
<td>dataplane</td>
<td>1-dataplane</td>
<td>No</td>
<td>293556</td>
<td>11</td>
</tr>
<tr>
<td>15310</td>
<td>switchdrvr</td>
<td>2-switchdrvr</td>
<td>No</td>
<td>177220</td>
<td>57</td>
</tr>
<tr>
<td>15314</td>
<td>syncdb</td>
<td>3-syncdb</td>
<td>No</td>
<td>2860</td>
<td>8</td>
</tr>
<tr>
<td>18718</td>
<td>lighttpd</td>
<td>4-lighttpd</td>
<td>No</td>
<td>5508</td>
<td>11</td>
</tr>
<tr>
<td>18720</td>
<td>lua_magnet</td>
<td>4-lighttpd</td>
<td>Yes</td>
<td>12112</td>
<td>7</td>
</tr>
<tr>
<td>18721</td>
<td>lua_magnet</td>
<td>4-lighttpd</td>
<td>Yes</td>
<td>25704</td>
<td>7</td>
</tr>
</tbody>
</table>

### 3.4.21 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.

---

**NOTICE**

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.

---

**NOTICE**

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.

---

**NOTICE**

If you use a text-based configuration file, the `show running-config` command only displays 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).

---

Use the following keys to navigate the command output.

<table>
<thead>
<tr>
<th>Key</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter</td>
<td>Advance one line.</td>
</tr>
<tr>
<td>Space Bar</td>
<td>Advance one page.</td>
</tr>
<tr>
<td>q</td>
<td>Stop the output and return to the prompt.</td>
</tr>
</tbody>
</table>
Note that --More-- or (q)uit is displayed at the bottom of the output screen until you reach the end of the output. 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

### 3.4.22 show running-config interface

Use this command to display the running configuration for a specific interface. Valid interfaces include physical, LAG, loopback, tunnel and VLAN interfaces.

**Format**

```
show running-config interface {interface | lag {lag-intf-num} | loopback {loopback-id} | tunnel {tunnel-id} | vlan {vlan-id}}
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Running configuration for the specified interface.</td>
</tr>
<tr>
<td>lag-intf-num</td>
<td>Running configuration for the LAG interface.</td>
</tr>
<tr>
<td>loopback-id</td>
<td>Running configuration for the loopback interface.</td>
</tr>
<tr>
<td>tunnel-id</td>
<td>Running configuration for the tunnel interface.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Running configuration for the VLAN routing interface.</td>
</tr>
</tbody>
</table>

The following information is displayed for the command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>port</td>
</tr>
<tr>
<td>lag</td>
<td>Display the running config for a specified lag interface.</td>
</tr>
<tr>
<td>loopback</td>
<td>Display the running config for a specified loopback interface.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Display the running config for a specified tunnel interface.</td>
</tr>
<tr>
<td>vlan</td>
<td>Display the running config for a specified vlan routing interface.</td>
</tr>
</tbody>
</table>

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

```
(Routing) #show running-config interface 0/1
Current Configuration:
!
interface 0/1
addport 3/1
exit
(Routing) #
```

### 3.4.23 show

This command displays the content of text-based configuration files from the CLI. The text-based configuration files (startup-config, backup-config and factory-defaults) are saved compressed in flash. With this command, the files are decompressed while displaying their content.

**Format**

```
show { startup-config | backup-config | factory-defaults }
```

**Mode**

Privileged EXEC
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>Display the content of the startup-config file.</td>
</tr>
<tr>
<td>backup-config</td>
<td>Display the content of the backup-config file.</td>
</tr>
<tr>
<td>factory-defaults</td>
<td>Display the content of the factory-defaults file.</td>
</tr>
</tbody>
</table>

**Example:** The following shows example CLI display output for the command using the startup-config parameter.

(Routing) # show startup-config

!Current Configuration:


!System Software Version "8.1.14.41"

!System Up Time "0 days 0 hrs 48 mins 19 secs"

!Cut-through mode is configured as disabled

!Additional Packages BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center

!Current SNTP Synchronized Time: Not Synchronized

! vlan database

! vlan 10

! exit

! configure

! ipv6 router ospf

! exit

! line console

! exit

! line telnet

! exit

! line ssh

! exit

! --More-- or (q)uit

! interface 0/1

! description 'intf1'

! exit

! router ospf

! exit

! exit

**Example:** The following shows example CLI display output for the command using the backup-config parameter.

(Routing) # show backup-config

!Current Configuration:


!System Software Version "8.1.14.41"

!System Up Time "0 days 0 hrs 48 mins 19 secs"

!Cut-through mode is configured as disabled

!Additional Packages BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center

!Current SNTP Synchronized Time: Not Synchronized

! vlan database

! vlan 10

! exit

! configure

! ipv6 router ospf

! exit

! line console

! exit

! line telnet

! exit

! line ssh

! exit
Example: The following shows example CLI display output for the command using the factory-defaults parameter.

```
(Routing) #show factory-defaults
Current Configuration:

System Software Version "8.1.14.41"
System Up Time "0 days 0 hrs 48 mins 19 secs"
Cut-through mode is configured as disabled
Additional Packages BGP-4,QoS,IPv6,IPv6 Management,Routing,Data Center

Current SNTP Synchronized Time: Not Synchronized

vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit

--More-- or (q)uit
```

3.4.24 dir

Use this command to list the files in the directory /mnt/fastpath in flash from the CLI.

```
Format dir
Mode Privileged EXEC

(Routing) #dir

  0 drwx  2048 May 09 2002 16:47:30 .
  0 drwx  2048 May 09 2002 16:45:28 ..
  0 -rwx  592 May 09 2002 14:50:24 slog2.txt
  0 -rwx  72 May 09 2002 16:45:28 boot.dim
  0 -rwx  0 May 09 2002 14:46:36 olog2.txt
  0 -rwx  13376020 May 09 2002 14:49:10 image1
  0 -rwx  0 Apr 06 2001 19:58:28 fsyssize
  0 -rwx  1776 May 09 2002 16:44:38 slog1.txt
  0 -rwx  356 Jun 17 2001 10:43:18 crashdump.ctl
  0 -rwx  1024 May 09 2002 16:45:44 ss1t.rnd
  0 -rwx  14328276 May 09 2002 16:01:06 image2
  0 -rwx  148 May 09 2002 16:46:06 hpc_broad.cfg
```
3.4.25 show sysinfo

This command displays switch information.

**Format**

```
show sysinfo
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Description</td>
<td>Text used to identify this switch.</td>
</tr>
<tr>
<td>System Name</td>
<td>Name used to identify the switch. The factory default is blank. To configure the system name, see &quot;snmp-server&quot; on page 71.</td>
</tr>
<tr>
<td>System Location</td>
<td>Text used to identify the location of the switch. The factory default is blank. To configure the system location, see &quot;snmp-server&quot; on page 71.</td>
</tr>
<tr>
<td>System Contact</td>
<td>Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see &quot;snmp-server&quot; on page 71.</td>
</tr>
<tr>
<td>System ObjectID</td>
<td>The base object ID for the switch’s enterprise MIB.</td>
</tr>
<tr>
<td>System Up Time</td>
<td>The time in days, hours and minutes since the last switch reboot.</td>
</tr>
<tr>
<td>Current SNTP Synchronized Time</td>
<td>The system time acquired from a network SNTP server.</td>
</tr>
<tr>
<td>MIBs Supported</td>
<td>A list of MIBs supported by this agent.</td>
</tr>
</tbody>
</table>

3.4.26 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 and includes log history files from previous runs:

- show version
- show sysinfo
- show port all
- show isdp neighbors
- show logging
- show event log
- show logging buffered
- show msg-queue
- show trap log
- show running-config

Including the optional `ospf` parameter also displays OSPF information.

**Format**

```
show tech-support [ospf|ospfv3|bfd]
```

**Mode**

Privileged EXEC
3.4.27  **length value**
Use this command to set the pagination length to value number of lines for the sessions specified by configuring on different Line Config modes (telnet/ssh/console) and is persistent.

Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

**Example:** *Length* command on Line Console mode applies for Serial Console session.

<table>
<thead>
<tr>
<th>Default</th>
<th>24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td><code>length value</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Line Config</td>
</tr>
</tbody>
</table>

3.4.27.1  no length value
Use this command to set the pagination length to the default value number of lines.

<table>
<thead>
<tr>
<th>Format</th>
<th><code>no length value</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Line Config</td>
</tr>
</tbody>
</table>

3.4.28  **terminal length**
Use this command to set the pagination length to *value* number of lines for the current session. This command configuration takes an immediate effect on the current session and is nonpersistent.

<table>
<thead>
<tr>
<th>Default</th>
<th>24 lines per page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td><code>terminal length value</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.4.28.1  no terminal length
Use this command to set the *value* to the length value configured on Line Config mode depending on the type of session.

<table>
<thead>
<tr>
<th>Format</th>
<th><code>no terminal length value</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.4.29  **show terminal length**
Use this command to display all the configured terminal length values.

<table>
<thead>
<tr>
<th>Format</th>
<th><code>show terminal length</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

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

(Routing) #show terminal length
Terminal Length:
-----------------
For Current Session.................. 24
For Serial Console................... 24
For Telnet Sessions................... 24
For SSH Sessions..................... 24
3.4.30 memory free low-watermark processor

Use this command to get notifications when the CPU free memory falls below the configured threshold. A notification is generated when the free memory falls below the threshold. Another notification is generated once the available free memory rises to 10 percent above the specified threshold. To prevent generation of excessive notifications when the CPU free memory fluctuates around the configured threshold, only one Rising or Falling memory notification is generated over a period of 60 seconds. The threshold is specified in kilobytes. The CPU free memory threshold configuration is saved across a switch reboot.

**Format**

```
memory free low-watermark processor 1-1034956
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>low-watermark</td>
<td>When CPU free memory falls below this threshold, a notification message is triggered. The range is 1 to the maximum available memory on the switch. The default is 0 (disabled).</td>
</tr>
</tbody>
</table>

3.4.31 clear mac-addr-table

Use this command to dynamically clear learned entries from the forwarding database. Using the following options, the user can specify the set of dynamically-learned forwarding database entries to clear.

**Default**

No default value.

**Format**

```
clear mac-addr-table {all | vlan vlanId | interface unit/slot/port | macAddr macMask}
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears dynamically learned forwarding database entries in the forwarding database table.</td>
</tr>
<tr>
<td>vlan vlanId</td>
<td>Clears dynamically learned forwarding database entries for this vlanId.</td>
</tr>
<tr>
<td>interface unit/slot/port</td>
<td>Clears forwarding database entries learnt on for the specified interface.</td>
</tr>
<tr>
<td>macAddr macMask</td>
<td>Clears dynamically learned forwarding database entries that match the range specified by MAC address and MAC mask. When MAC mask is not entered, only specified MAC is removed from the forwarding database table.</td>
</tr>
</tbody>
</table>

3.5 Logging Commands

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

3.5.1 logging buffered

This command enables logging to an in-memory log.

**Default**

disabled; critical when enabled

**Format**

```
logging buffered
```

**Mode**

Global Config
3.5.1.1 no logging buffered
This command disables logging to in-memory log.

Format: no logging buffered
Mode: Global Config

3.5.2 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

3.5.2.1 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

3.5.3 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. The commands are stored in a persistent log. Use the show logging persistent command to display the stored history of CLI commands.

Default: enabled
Format: logging cli-command
Mode: Global Config

3.5.3.1 no logging cli-command
This command disables the CLI command Logging feature.

Format: no logging cli-command
Mode: Global Config

3.5.4 logging console
This command enables logging to the console. You can specify the severity level 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 [severity level]
Mode: Global Config
3.5.4.1 no logging console
This command disables logging to the console.

Format
no logging console
Mode
Global Config

3.5.5 logging host
This command configures the logging host parameters. You can configure up to eight hosts.

Default
- port: 514 (for UDP) and 6514 (for TLS)
- authentication mode: anonymous
- certificate index: 0
- level: critical (2)

Format
logging host {hostaddress|hostname} addresstype {tls [anon|x509name] certificate-index {port severitylevel}
Mode
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostaddress</td>
<td>hostname</td>
</tr>
<tr>
<td>address-type</td>
<td>Indicates the type of address being passed: DNS or IPv4.</td>
</tr>
<tr>
<td>tls</td>
<td>Enables TLS security for the host.</td>
</tr>
<tr>
<td>anon</td>
<td>x509name</td>
</tr>
<tr>
<td>certificate-index</td>
<td>The certificate number to be used for authentication. The valid range is 0–8. Index 0 is used to the default file.</td>
</tr>
<tr>
<td>port</td>
<td>A port number from 1 to 65535.</td>
</tr>
<tr>
<td>severitylevel</td>
<td>Specify this 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).</td>
</tr>
</tbody>
</table>

Example: The following shows examples of the command.
The following shows examples of the command.
(Routing) (Config)# logging host google.com dns 214
(Routing) (Config)# logging host 10.130.64.88 ipv4 214 6
(Routing) (Config)# logging host 5.5.5.5 ipv4 tls anon 6514 debug
(Routing) (Config)# logging host 5.5.5.5 ipv4 tls x509name 3 651

3.5.6 logging host reconfigure
This command enables logging host reconfiguration.

Format
logging host reconfigure hostindex
Mode
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostindex</td>
<td>Enter the Logging Host Index for which to change the IP address.</td>
</tr>
</tbody>
</table>
3.5.7 logging host remove
This command disables logging to host. See "show logging hosts" on page 146 for a list of host indexes.

Format logging host remove hostindex
Mode Global Config

3.5.8 logging protocol
Use this command to configure the logging protocol version number as 0 or 1. RFC 3164 uses version 0 and RFC 5424 uses version 1.

Default The default is version 0 (RFC 3164).
Format logging protocol {0|1}
Mode Global Config

3.5.9 logging syslog
This command enables syslog logging.

Format logging syslog
Mode Global Config

3.5.9.1 no logging syslog
This command disables syslog logging.

Format no logging syslog
Mode Global Config

3.5.10 logging syslog port
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

3.5.10.1 no logging syslog port
This command disables syslog logging.

Format no logging syslog port
Mode Global Config
3.5.11 logging syslog source-interface

This command configures the syslog source-interface (source IP address) for syslog server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

**Format**

```
logging syslog source-interface {slot/port}|{loopback loopback-id}|{vlan vlan-id}
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>VLAN or port-based routing interface.</td>
</tr>
<tr>
<td>loopback-id</td>
<td>Configures the loopback interface to use as the source IP address. The range of the loopback ID is 0 to 7.</td>
</tr>
<tr>
<td>tunnel-id</td>
<td>Configures the tunnel interface to use as the source IP address. The range of the tunnel ID is 0 to 7.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.</td>
</tr>
</tbody>
</table>

**Example:** The following shows examples of the command.

```
(config)#logging syslog source-interface loopback 0
(config)#logging syslog source-interface tunnel 0
(config)#logging syslog source-interface 0/4/1
(config)#logging syslog source-interface 0/1
```

3.5.11.1 no logging syslog source-interface

This command disables syslog logging.

**Format**

```
no logging syslog
```

**Mode**

Global Config

3.5.12 show logging

This command displays logging configuration information.

**Format**

```
show logging
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Client Local Port</td>
<td>Port on the collector/relay to which syslog messages are sent.</td>
</tr>
<tr>
<td>Logging Client Source Interface</td>
<td>Shows the configured syslog source-interface (source IP address).</td>
</tr>
<tr>
<td>CLI Command Logging</td>
<td>Shows whether CLI Command logging is enabled.</td>
</tr>
<tr>
<td>Logging Protocol</td>
<td>The logging protocol version number.</td>
</tr>
<tr>
<td></td>
<td>• 0: RFC 3164</td>
</tr>
<tr>
<td></td>
<td>• 1: RFC 5424</td>
</tr>
<tr>
<td>Console Logging</td>
<td>Shows whether console logging is enabled.</td>
</tr>
<tr>
<td>Console Logging Severity Filter</td>
<td>The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.</td>
</tr>
</tbody>
</table>
3.5.13 show logging buffered

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

**Format**

```
show logging buffered
```

**Mode**

Privileged EXEC

---

**Table: Term vs. Definition**

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

---

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

(Routing) #show logging

```
Logging Client Local Port : 514
Logging Client Source Interface : (not configured)
CLI Command Logging : disabled
Logging Protocol : 1
Console Logging : enabled
Console Logging Severity Filter : error
Buffered Logging : enabled
Persistent Logging : disabled
Persistent Logging Severity Filter : alert

Syslog Logging : disabled

Log Messages Received : 1010
Log Messages Dropped : 0
Log Messages Relayed : 0
```
3.5.14  show logging hosts

This command displays all configured logging hosts. Use the "|" character to display the output filter options.

Format  show logging hosts
Mode Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Index</td>
<td>(Used for deleting hosts.)</td>
</tr>
<tr>
<td>IP Address / Hostname</td>
<td>IP address or hostname of the logging host.</td>
</tr>
<tr>
<td>Severity Level</td>
<td>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).</td>
</tr>
<tr>
<td>Port</td>
<td>The server port number, which is the port on the local host from which syslog messages are sent.</td>
</tr>
<tr>
<td>Status</td>
<td>Status field provides the current status of snmp row status. (Active, Not in Service, Not Ready).</td>
</tr>
<tr>
<td>Mode</td>
<td>The type of security: UDP or TLS.</td>
</tr>
<tr>
<td>Auth</td>
<td>The type of authentication mode: anonymous or x509name.</td>
</tr>
<tr>
<td>Cert #</td>
<td>The certificate number to be used for authentication. The valid range is 0–8. Index 0 is used to the default file.</td>
</tr>
</tbody>
</table>

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

(Routing) #show logging hosts

<table>
<thead>
<tr>
<th>Index</th>
<th>IP Address/Hostname</th>
<th>Severity</th>
<th>Port</th>
<th>Status</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1.1.17</td>
<td>critical</td>
<td>514</td>
<td>Active</td>
<td>udp</td>
</tr>
<tr>
<td>2</td>
<td>10.130.191.90</td>
<td>debug</td>
<td>10514</td>
<td>Active</td>
<td>tls</td>
</tr>
<tr>
<td>3</td>
<td>5.5.5.5</td>
<td>debug</td>
<td>333</td>
<td>Active</td>
<td>tls</td>
</tr>
</tbody>
</table>

Auth Cert#
-------- -----
x509name 6
x509name 4

3.5.15  show logging persistent

Use the show logging persistent command to display persistent log entries. If log-files is specified, the system persistent log files are displayed.

Format  show logging persistent [log-files]
Mode Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent Logging</td>
<td>If persistent logging is enabled or disabled.</td>
</tr>
<tr>
<td>Persistent Log Count</td>
<td>The number of persistent log entries.</td>
</tr>
<tr>
<td>Persistent Log Files</td>
<td>The list of persistent log files in the system. Only displayed if log-files is specified.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(FASTPATH Switching) #show logging persistent

Persistent Logging : disabled
Persistent Log Count : 0

(FASTPATH Switching) #show logging persistent log-files

Persistent Log Files:

slog0.txt
slog1.txt
slog2.txt
olog0.txt
olog1.txt
olog2.txt

3.5.16 show logging traplogs

This command displays SNMP trap events and statistics.

**Format**

show logging traplogs

**Mode**

Privileged EXEC

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

3.5.17 clear logging buffered

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

**Format**

clear logging buffered

**Mode**

Privileged EXEC

3.6 Email Alerting and Mail Server Commands

3.6.1 logging email

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires. 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; when enabled, log messages at or above severity Warning (4) are emailed

**Format**

logging email [severityLevel]

**Mode**

Global Config
3.6.1.1 no logging email
This command disables email alerting.

**Format**
```
no logging email
```

**Mode**
Global Config

3.6.2 logging email urgent
This command sets the lowest severity level at which log messages are emailed immediately in a single email message. 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). Specify `none` to indicate that log messages are collected and sent in a batch email at a specified interval.

**Default**
Alert (1) and emergency (0) messages are sent immediately.

**Format**
```
logging email urgent {severityLevel | none}
```

**Mode**
Global Config

3.6.2.1 no logging email urgent
This command resets the urgent severity level to the default value.

**Format**
```
no logging email urgent
```

**Mode**
Global Config

3.6.3 logging email message-type to-addr
This command configures the email address to which messages are sent. The message types supported are `urgent`, `non-urgent`, and `both`. For each supported severity level, multiple email addresses can be configured. The `to-email-addr` variable is a standard email address, for example admin@yourcompany.com.

**Format**
```
logging email message-type {urgent | non-urgent | both} to-addr to-email-addr
```

**Mode**
Global Config

3.6.3.1 no logging email message-type to-addr
This command removes the configured to-addr field of email.

**Format**
```
no logging email message-type {urgent | non-urgent | both} to-addr to-email-addr
```

**Mode**
Global Config

3.6.4 logging email from-addr
This command configures the email address of the sender (the switch).

**Default**
```
switch@broadcom.com
```

**Format**
```
logging email from-addr from-email-addr
```

**Mode**
Global Config
3.6.4.1 no logging email from-addr
This command removes the configured email source address.

**Format**
```
no logging email from-addr from-email-addr
```

**Mode**
Global Config

3.6.5 logging email message-type subject
This command configures the subject line of the email for the specified type.

**Default**
For urgent messages: Urgent Log Messages
For non-urgent messages: Non Urgent Log Messages

**Format**
```
logging email message-type {urgent | non-urgent | both} subject subject
```

**Mode**
Global Config

3.6.5.1 no logging email message-type subject
This command removes the configured email subject for the specified message type and restores it to the default email subject.

**Format**
```
no logging email message-type {urgent | non-urgent | both} subject
```

**Mode**
Global Config

3.6.6 logging email logtime
This command configures how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval. The valid range is every 30–1440 minutes.

**Default**
30 minutes

**Format**
```
logging email logtime minutes
```

**Mode**
Global Config

3.6.6.1 no logging email logtime
This command resets the non-urgent log time to the default value.

**Format**
```
no logging email logtime
```

**Mode**
Global Config

3.6.7 logging traps
This command sets the severity at which SNMP traps are logged and sent in an email. 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**
Info (6) messages and higher are logged.

**Format**
```
logging traps severityLevel
```

**Mode**
Global Config
3.6.7.1  no logging traps
This command resets the SNMP trap logging severity level to the default value.

**Format**  no logging traps
**Mode**  Global Config

3.6.8  logging email test message-type
This command sends an email to the SMTP server to test the email alerting function.

**Format**  logging email test message-type {urgent | non-urgent | both} message-body message-body
**Mode**  Global Config

3.6.9  show logging email config
This command displays information about the email alert configuration.

**Format**  show logging email config
**Mode**  Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Alert Logging</td>
<td>The administrative status of the feature: enabled or disabled</td>
</tr>
<tr>
<td>Email Alert From Address</td>
<td>The email address of the sender (the switch).</td>
</tr>
<tr>
<td>Email Alert Urgent Severity Level</td>
<td>The lowest severity level that is considered urgent. Messages of this type are sent immediately.</td>
</tr>
<tr>
<td>Email Alert Non Urgent Severity Level</td>
<td>The lowest severity level that is considered non-urgent. Messages of this type, up to the urgent level, are collected and sent in a batch email. Log messages that are less severe are not sent in an email message at all.</td>
</tr>
<tr>
<td>Email Alert Trap Severity Level</td>
<td>The lowest severity level at which traps are logged.</td>
</tr>
<tr>
<td>Email Alert Notification Period</td>
<td>The amount of time to wait between non-urgent messages.</td>
</tr>
<tr>
<td>Email Alert To Address Table</td>
<td>The configured email recipients.</td>
</tr>
<tr>
<td>Email Alert Subject Table</td>
<td>The subject lines included in urgent (Type 1) and non-urgent (Type 2) messages.</td>
</tr>
<tr>
<td>For Msg Type urgent, subject is</td>
<td>The configured email subject for sending urgent messages.</td>
</tr>
<tr>
<td>For Msg Type non-urgent, subject is</td>
<td>The configured email subject for sending non-urgent messages.</td>
</tr>
</tbody>
</table>

3.6.10  show logging email statistics
This command displays email alerting statistics.

**Format**  show logging email statistics
**Mode**  Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Alert Operation Status</td>
<td>The operational status of the email alerting feature.</td>
</tr>
<tr>
<td>No of Email Failures</td>
<td>The number of email messages that have attempted to be sent but were unsuccessful.</td>
</tr>
</tbody>
</table>
3.6.11 clear logging email statistics

This command resets the email alerting statistics.

<table>
<thead>
<tr>
<th>Format</th>
<th>clear logging email statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.6.12 mail-server

This command configures the SMTP server to which the switch sends email alert messages and changes the mode to Mail Server Configuration mode. The server address can be in the IPv4, IPv6, or DNS name format.

| Format                  | mail-server {ip-address | ipv6-address | hostname} |
|-------------------------|-----------------------------------------------|
| Mode                    | Global Config                                |

3.6.12.1 no mail-server

This command removes the specified SMTP server from the configuration.

| Format                  | no mail-server {ip-address | ipv6-address | hostname} |
|-------------------------|--------------------------------------------------|
| Mode                    | Global Config                                  |

3.6.13 security

This command sets the email alerting security protocol by enabling the switch to use TLS authentication with the SMTP Server. If the TLS mode is enabled on the switch but the SMTP server does not support TLS mode, no email is sent to the SMTP server.

<table>
<thead>
<tr>
<th>Default</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>security {tlsv1</td>
</tr>
<tr>
<td>Mode</td>
<td>Mail Server Config</td>
</tr>
</tbody>
</table>

3.6.14 port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, and for no security (i.e. none) it is 25. However, any nonstandard port in the range 1 to 65535 is also allowed.

<table>
<thead>
<tr>
<th>Default</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>port (465</td>
</tr>
<tr>
<td>Mode</td>
<td>Mail Server Config</td>
</tr>
</tbody>
</table>
### 3.6.15 username (Mail Server Config)
This command configures the login ID the switch uses to authenticate with the SMTP server.

**Default**
admin

**Format**
```
username name
```

**Mode**
Mail Server Config

### 3.6.16 password
This command configures the password the switch uses to authenticate with the SMTP server.

**Default**
admin

**Format**
```
password password
```

**Mode**
Mail Server Config

### 3.6.17 show mail-server config
This command displays information about the email alert configuration.

**Format**
```
show mail-server {ip-address | hostname | all} config
```

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of mail servers configured</td>
<td>The number of SMTP servers configured on the switch.</td>
</tr>
<tr>
<td>Email Alert Mail Server Address</td>
<td>The IPv4/IPv6 address or DNS hostname of the configured SMTP server.</td>
</tr>
<tr>
<td>Email Alert Mail Server Port</td>
<td>The TCP port the switch uses to send email to the SMTP server</td>
</tr>
<tr>
<td>Email Alert Security Protocol</td>
<td>The security protocol (TLS or none) the switch uses to authenticate with the SMTP server.</td>
</tr>
<tr>
<td>Email Alert Username</td>
<td>The username the switch uses to authenticate with the SMTP server.</td>
</tr>
<tr>
<td>Email Alert Password</td>
<td>The password the switch uses to authenticate with the SMTP server.</td>
</tr>
</tbody>
</table>

### 3.7 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.

#### 3.7.1 traceroute
Use the **traceroute** command to discover the routes that IPv4 or IPv6 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.

The user may specify the source IP address or the virtual router of the traceroute probes. Recall that traceroute works by sending packets that are expected not to reach their final destination, but instead trigger ICMP error messages back to the source address from each hop along the forward path to the destination. By specifying the source address, the user can determine where along the forward path there is no route back to the source address. Note that this is only useful if the route from source to destination and destination to source is symmetric. It would be common, for example, to send a traceroute from an edge router to a target higher in the network using a source address from a host subnet on the edge router. This would test reachability from within the network back to hosts attached to the edge router. Alternatively, one might send a traceroute with an address on a loopback interface as a source to test reachability back to the loopback interface address.
In the CLI, the user may specify the source as an IPv4 address, IPv6 address, a virtual router, or as a routing interface. When the source is specified as a routing interface, the traceroute is sent using the primary IPv4 address on the source interface. With SNMP, the source must be specified as an address. The source cannot be specified in the web UI.

FASTPATH will not accept an incoming packet, such as a traceroute response, that arrives on a routing interface if the packet's destination address is on one of the out-of-band management interfaces (service port or network port). Similarly, FASTPATH will not accept a packet that arrives on a management interface if the packet's destination is an address on a routing interface. Thus, it would be futile to send a traceroute on a management interface using a routing interface address as source, or to send a traceroute on a routing interface using a management interface as source. When sending a traceroute on a routing interface, the source must be that routing interface or another routing interface. When sending a traceroute on a management interface, the source must be on that management interface. For this reason, the user cannot specify the source as a management interface or management interface address. When sending a traceroute on a management interface, the user should not specify a source address, but instead let the system select the source address from the outgoing interface.

**Default**
- count: 3 probes
- interval: 3 seconds
- size: 0 bytes
- port: 33434
- maxTtl: 30 hops
- maxFail: 5 probes
- initTtl: 1 hop

**Format**
```
traceroute {ip-address | [ipv6] {ipv6-address | hostname}} [initTtl initTtl] [maxTtl maxTtl] [maxFail maxFail] [interval interval] [count count] [port port] [size size] [source {ip-address | | ipv6-address | slot/port}]
```

**Mode**
Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>The ipaddress value should be a valid IP address.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>The ipv6-address value should be a valid IPv6 address.</td>
</tr>
<tr>
<td>hostname</td>
<td>The hostname value should be a valid hostname.</td>
</tr>
<tr>
<td>ipv6</td>
<td>The optional ipv6 keyword can be used before ipv6-address or hostname. Giving the ipv6 keyword before the hostname tries it to resolve to an IPv6 address.</td>
</tr>
<tr>
<td>initTtl</td>
<td>Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.</td>
</tr>
<tr>
<td>maxTtl</td>
<td>Use maxTtl to specify the maximum TTL. Range is 1 to 255.</td>
</tr>
<tr>
<td>maxFail</td>
<td>Use maxFail to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.</td>
</tr>
<tr>
<td>interval</td>
<td>Use the optional interval parameter to specify the time between probes, in seconds. If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.</td>
</tr>
<tr>
<td>count</td>
<td>Use the optional count parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.</td>
</tr>
<tr>
<td>port</td>
<td>Use the optional port parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.</td>
</tr>
<tr>
<td>size</td>
<td>Use the optional size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.</td>
</tr>
<tr>
<td>source</td>
<td>Use the optional source parameter to specify the source IP address or interface for the traceroute.</td>
</tr>
</tbody>
</table>
The following are examples of the CLI command.

**Example: traceroute Success:**

(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 ipv6 Success**

(Routing) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1 2001::2 708 msec 41 msec 11 msec

The above command can also be execute with the optional ipv6 parameter as follows:

(Routing) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size 43

**Example: traceroute Failure:**

(Routing) # traceroute 10.40.1.1 initTtl 1 maxTtl 0 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

**Example: traceroute ipv6 Failure**

(Routing) # traceroute ipv6 2001::2 initTtl 1 maxTtl 0 maxFail 0 interval 1 count 3 port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1 3001::1 708 msec 41 msec 11 msec
2 4001::2 250 msec 200 msec 193 msec
3 5001::3 289 msec 313 msec 278 msec
4 6001::4 651 msec 41 msec 270 msec
5 0 0 msec *

Hop Count = 4 Last TTL = 5 Test attempt = 1 Test Success = 0

### 3.7.2 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.

**Format**

```
clear config
```  

**Mode**

Privileged EXEC
3.7.3 clear config interface

This command resets the configuration in the specified interface or range of interfaces 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 interface or interfaces to the default values. It does not reset the switch.

The clear config interface command clears the configuration only for commands issued in Interface Config mode. Interface-related commands which were not issued in Interface Config mode, such as enabling routing on a VLAN interface, cannot be cleared using this command.

Format clear config interface {slot/port | lag lag_id | vlan vlan_id | loopback loopback_id}
Mode Privileged EXEC

3.7.4 clear counters

This command clears the statistics for a specified slot/port, for all the ports, or for an interface on a VLAN based on the argument, including the loop protection counters.

Format clear counters {slot/port | all | vlan id}
Mode Privileged EXEC

3.7.5 clear igmpsnooping

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

Format clear igmpsnooping
Mode Privileged EXEC

3.7.6 clear ip access-list counters

This command clears the counters of the specified IP ACL and IP ACL rule.

Format clear ip access-list counters acl-ID | acl-name rule-id
Mode Privileged EXEC

3.7.7 clear ipv6 access-list counters

This command clears the counters of the specified IP ACL and IP ACL rule.

Format clear ipv6 access-list counters acl-name rule-id
Mode Privileged EXEC

3.7.8 clear mac access-list counters

This command clears the counters of the specified MAC ACL and MAC ACL rule.

Format clear mac access-list counters acl-name rule-id
Mode Privileged EXEC
3.7.9 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

3.7.10 clear traplog
This command clears the trap log.

**Format**
clear traplog

**Mode**
Privileged EXEC

3.7.11 clear vlan
This command resets VLAN configuration parameters to the factory defaults. When the VLAN configuration is reset to the factory defaults, there are some scenarios regarding GVRP that happen due to this:

1. **Static VLANs are deleted.**
2. **GVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event.** Since GVRP is disabled by default, this means that GVRP should be disabled and all of its dynamic VLANs should be deleted.
3. **MVRP is restored to the factory default as a result of handling the VLAN RESTORE NOTIFY event.** Since MVRP is enabled by default, this means that any VLANs already created by MVRP are unaffected. However, for customer platforms where MVRP is disabled by default, then the MVRP behavior should match GVRP. That is, MVRP is disabled and the MVRP VLANs are deleted.

**Format**
clear vlan

**Mode**
Privileged EXEC

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

---

Save configuration changes before logging out.

---

**Format**
logout

**Modes**
- Privileged EXEC
- User EXEC

3.7.13 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.

---

For information about the ping command for IPv6 hosts, see “ping ipv6” on page 649.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>IPv4 or IPv6 addresses to ping.</td>
</tr>
<tr>
<td>count</td>
<td>Use the count parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the ip-address field. The range for count is 1 to 15 requests.</td>
</tr>
<tr>
<td>interval</td>
<td>Use the interval parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.</td>
</tr>
<tr>
<td>size</td>
<td>Use the size parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.</td>
</tr>
<tr>
<td>source</td>
<td>Use the source parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.</td>
</tr>
<tr>
<td>hostname</td>
<td>Use the hostname parameter to resolve to an IPv4 or IPv6 address. The ipv6 keyword is specified to resolve the hostname to IPv6 address. The IPv4 address is resolved if no keyword is specified.</td>
</tr>
<tr>
<td>ipv6</td>
<td>The optional keyword ipv6 can be used before the ipv6-address or hostname argument. Using the ipv6 optional keyword before hostname tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.</td>
</tr>
<tr>
<td>interface</td>
<td>Use the interface keyword to ping a link-local IPv6 address over an interface.</td>
</tr>
<tr>
<td>link-local-address</td>
<td>The link-local IPv6 address to ping over an interface.</td>
</tr>
</tbody>
</table>

The following are examples of the CLI command.

**Example:** IPv4 ping success:
(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:** IPv6 ping success
(FASTPATH Routing) # ping 2001::1
Pinging 2001::1 with 64 bytes of data:

Send count=3, Receive count=3 from 2001::1
Average round trip time = 3.00 ms

**Example:** IPv4 ping failure:
In Case of Unreachable Destination:

(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

In Case Of Request TimedOut:

(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

Example: IPv6 ping failure
(FASTPATH Routing) #ping ipv6 2001::4
Pinging 2001::4 with 64 bytes of data:
Send count=3, Receive count=0 from 2001::4
Average round trip time = 0.00 ms

3.7.14 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

3.7.15 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 [configuration [scriptname]]
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>Gracefully reloads the configuration. If no configuration file is specified, the startup-config file is loaded.</td>
</tr>
<tr>
<td>scriptname</td>
<td>The configuration file to load. The scriptname must include the extension.</td>
</tr>
</tbody>
</table>
3.7.16 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 (active and backup) on the file system. Upload and download files from a server using FTP, TFTP, Xmodem, Ymodem, or Zmodem.

**NOTICE**

Please note, the low security SW version does support neither ssh, scp, sftp and https nor Crypto key generation.

SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

**Format**

```
copy source destination {verify | novery}
```

**Mode**

Privileged EXEC

Replace the source and destination parameters with the options in Table 9 on page 160. For the url source or destination, use one of the following values:

{ xmodem | tftp://ipaddr|hostname | ipaddress|hostname/filepath|filename [noval] } sftp|scp:// username@ipaddr | ipv6address/filepath|filename | ftp://user@ipaddress | hostname/filepath/ filename}

*verify* | *noverify* is only available if the image/configuration verify options feature is enabled (see "file verify" on page 166). *verify* specifies that digital signature verification will be performed for the specified downloaded image or configuration file. *noverify* specifies that no verification will be performed.

The keyword ias-users supports the downloading of the IAS user database file. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and its attributes available in the downloaded file. In the command copy url ias-users, for url one of the following is used for IAS users file:

{ { tftp://<ipaddr | hostname> | <ipv6address | hostname> /<filepath>/<filename> } | { sftp | scp://<username>@<ipaddress>/<filepath>/<filename>} }  

The maximum length for the file path is 160 characters, and the maximum length for the file name is 31 characters.

For FTP, 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.

**NOTICE**

*ip6address* is also a valid parameter for routing packages that support IPv6.

To copy OpenFlow SSL certificates to the switch using TFTP or XMODEM, using only the following options pertinent to the OpenFlow SSL certificates.

**Format**

```
copy [<mode/file>] nvram:{openflow-ssl-ca-cert | openflow-ssl-cert | openflow-ssl-priv-key}
```

**Mode**

Privileged EXEC

**CAUTION**

Remember to upload the existing fastpath.cfg file of the switch prior to loading a new release image in order to make a backup.
### Table 9: Copy Parameters

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nvram:backup-config</td>
<td>nvram:startup-config</td>
<td>Copies the backup configuration to the startup configuration.</td>
</tr>
<tr>
<td>nvram:clibanner</td>
<td>url</td>
<td>Copies the CLI banner to a server.</td>
</tr>
<tr>
<td>nvram:core-dump</td>
<td>tftp://&lt;ipaddress</td>
<td>hostnam&lt;/path&gt;/&lt;filename&gt;</td>
</tr>
<tr>
<td>nvram:cpupktcapture.pcap</td>
<td>url</td>
<td>Uploads CPU packets capture file.</td>
</tr>
<tr>
<td>nvram:crash-log</td>
<td>url</td>
<td>Copies the crash log to a server.</td>
</tr>
<tr>
<td>nvram:errorlog</td>
<td>url</td>
<td>Copies the error log file to a server.</td>
</tr>
<tr>
<td>nvram:factory-defaults</td>
<td>url</td>
<td>Uploads factory defaults file.</td>
</tr>
<tr>
<td>nvram:fastpath.cfg</td>
<td>url</td>
<td>Uploads the config file to a server.</td>
</tr>
<tr>
<td>nvram:log</td>
<td>url</td>
<td>Copies the log file to a server.</td>
</tr>
<tr>
<td>nvram:file</td>
<td>url</td>
<td>Uploads a specified file.</td>
</tr>
<tr>
<td>nvram:factory-all</td>
<td>url</td>
<td>Copy all factory settings.</td>
</tr>
<tr>
<td>nvram:oslog</td>
<td>url</td>
<td>Copies the OS system log file to a server.</td>
</tr>
<tr>
<td>nvram:operational-log</td>
<td>url</td>
<td>Copies the operational log file to a server.</td>
</tr>
<tr>
<td>nvram:script scriptname</td>
<td>url</td>
<td>Copies a specified configuration script file to a server.</td>
</tr>
<tr>
<td>nvram:startup-config</td>
<td>nvram:backup-config</td>
<td>Copies the startup configuration to the backup configuration.</td>
</tr>
<tr>
<td>nvram:startup-config</td>
<td>url</td>
<td>Copies the startup configuration to a server.</td>
</tr>
<tr>
<td>nvram:startup-log</td>
<td>url</td>
<td>Uploads the startup log file.</td>
</tr>
<tr>
<td>nvram:traplog</td>
<td>url</td>
<td>Copies the trap log file to a server.</td>
</tr>
<tr>
<td>system:running-config</td>
<td>nvram:startup-config</td>
<td>Saves the running configuration to NVRAM.</td>
</tr>
<tr>
<td>system:running-config</td>
<td>nvram:factory-defaults</td>
<td>Saves the running configuration to NVRAM to the factory-defaults file.</td>
</tr>
<tr>
<td>system:image</td>
<td>url</td>
<td>Saves the system image to a server.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:application destfilename</td>
<td>Destination file name for the application file.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:clibanner</td>
<td>Downloads the CLI banner to the system.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:fastpath.cfg</td>
<td>Downloads the binary config file to the system.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:publickey-config</td>
<td>Downloads the Public Key for Configuration Script validation.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:publickey-image</td>
<td>Downloads Public Key for Image validation.</td>
</tr>
</tbody>
</table>
Table 9: Copy Parameters (Continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>nvram:script</td>
<td>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.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:script destfilename noval</td>
<td>When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows: (FASTPATH Routing) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval</td>
</tr>
<tr>
<td>url</td>
<td>nvram:sshkey-dsa</td>
<td>Downloads an SSH key file. For more information, see “Secure Shell Commands” on page 33.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:sshkey-rsa1</td>
<td>Downloads an SSH key file.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:sshkey-rsa2</td>
<td>Downloads an SSH key file.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:sslpm-dhweak</td>
<td>Downloads an HTTP secure-server certificate.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:sslpm-dhstrong</td>
<td>Downloads an HTTP secure-server certificate. For more information, see “Hypertext Transfer Protocol Commands” on page 37.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:sslpm-root</td>
<td>Downloads an HTTP secure-server certificate.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:sslpm-server</td>
<td>Downloads an HTTP secure-server certificate.</td>
</tr>
<tr>
<td>url</td>
<td>nvram:startup-config</td>
<td>Downloads the startup configuration file to the system.</td>
</tr>
<tr>
<td>url</td>
<td>ias-users</td>
<td>Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user’s database is replaced with the users and their attributes available in the downloaded file.</td>
</tr>
<tr>
<td>url</td>
<td>{active</td>
<td>backup}</td>
</tr>
<tr>
<td>url</td>
<td>nvram:file</td>
<td>Downloads a specified file</td>
</tr>
<tr>
<td>url</td>
<td>nvram:oem-data</td>
<td>Downloads and updates OEM data.</td>
</tr>
<tr>
<td>active</td>
<td>backup</td>
<td>Copy the active image to the backup image.</td>
</tr>
<tr>
<td>backup</td>
<td>active</td>
<td>Copy the backup image to the active image.</td>
</tr>
</tbody>
</table>

Example: The following shows an example of downloading and applying ias users file. (FASTPATH Routing) #copy tftp://10.131.17.104/aaa_users.txt ias-users

Mode........................................... TFTP
Set Server IP................................. 10.131.17.104
Path........................................... /
Filename....................................... aaa_users.txt
Data Type.................................... IAS Users

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
Validating and updating the users to the IAS users database.
Updated IAS users database successfully.

(FASTPATH Routing) #
3.7.17 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 Privilaged EXEC

3.7.17.1 no set bootstopkey
This command resets the bootstop key. The boot process can not be interrupted.

Format no set bootstopkey
Mode Privilaged EXEC

3.7.18 set board root-password
This command changes the current LINUX root password. The user will be asked by a prompt to specify the password and to reconfirm it a second time. An empty password can be specified by simply type <CR>. Then any password may be specified for the login. The factory password can be reconfigured (parameter 'factory').

Format set board root-password [factory]
Mode Privilaged EXEC

3.7.19 set board port-map
The command selects a specific port-map. It is used for boards where more than one port configuration is available related to e.g. the chassis or the RTM the board is used with. Various port configurations are pre-defined and can be selected via a number or a name (related to FASTPATH version). The "no" command is used to specify the default configuration.

Note that you have to save the specified configuration and reboot the system if the new configuration should become active!

Format set board port-map <name>
Mode Privilaged EXEC
3.7.19.1 no set board port-map
The command is used to specify the default configuration.

Format: `no set board port-map <name>`
Mode: Privileged EXEC

3.7.20 show board port-map
The command displays the selected port-map number.

Format: `show board port-map [selected]`
Mode: Privileged EXEC

3.7.21 show board port-map list
The command displays all available port-maps together with a description. The currently active port-map is marked.

Format: `show board port-map list`
Mode: Privileged EXEC

3.7.22 show board port-map descr
The command displays the description for all physical ports related to the currently selected port-map.

Format: `show board port-map descr`
Mode: Privileged EXEC

3.7.23 show board port-map all
The command displays all available port-maps together with a description. The currently active port-map is marked.

Format: `show board port-map all`
Mode: Privileged EXEC

3.7.24 show board address
This command displays the global address info of the board.

Format: `show board address`
Mode: Privileged EXEC
3.7.25 show board 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 board cpu-load
Mode Privileged EXEC

3.7.26 show board memory-usage
This command displays the Memory Usage. It shows malloc and kernel statistics.

Format show board memory-usage
Mode Privileged EXEC

3.7.27 show board post-status
This command displays the power on self test status of the board. It checks the status of the system selftest and the IPMC selftest.

Format show board post-status [system]
Mode Privileged EXEC

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

Format show board version [basic | hardware | release | all]
Mode Privileged EXEC

- Basic version information ("show board version" and "show board version basic")
- System description
- Board name
- Board serial number, part number and manufacturer
- Product serial number, part number and manufacturer
- FASTPATH version
- Hardware version information ("show board version hardware")
- Broadcom silicon
- Processor CPU type
- Processor clock
- Jumper settings (optional)
- PCB revision (optional)
- PLD revision (optional)
- PHY 10G type and firmware version
- Updatable firmware releases ("show board version release")
- System (FASTPATH) release
For "show board version all" all information is displayed.
3.7.29 show logging errcounter
This command displays the trace of the error counters.

**Format**      
show logging errcounter

**Mode**          
Privileged EXEC

3.7.30 clear errcounter
This command clears the error counters trace.

**Format**      
 clear errcounter

**Mode**          
Privileged EXEC

3.7.31 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

3.7.32 set board sensor threshold
This command sets a new threshold value for a sensor. The ‘sensor-number’ for a specific sensor is described (and displayed) in the “show” command. The value type is ‘float’.

The command sets the minimal or maximal threshold.

Note, that if a maximal hysteresis is supported by the sensor and the maximal threshold value is set, then the hysteresis value is set with the same amount the new value is incremented/decremented.

**Format**      
set board sensor threshold <sensor-number> [minimal | maximal] <value>

**Mode**          
Privileged EXEC
3.7.32.1 no set board sensor
With the 'no' command, the default value is set.

Format: no set board sensor threshold <sensor-number> [minimal | maximal]
Mode: Priviledged EXEC

3.7.33 show board sensors
This command displays the current sensor readings.

With parameter 'all' a common list of all sensors and types is displayed. Fields are a number, sensor name, current value, unit and status (ok, not-healthy, n/a or failed if not readable). The number consist of a unit number (only for stacking), a slot identifier and a internal sensor number delimited by a '/' character.

With parameter 'slot' a list of available slots and the related type of the source (Board, chip) is displayed.

With specifying a <number> detailed infos for this sensor related to the source are indicated.

Format: show board[info] sensors {all | slot | <number>}
Mode: Priviledged EXEC

3.7.34 file verify
This command enables digital signature verification while an image and/or configuration file is downloaded to the switch.

Format: file verify {all | image | none | script}
Mode: Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Verifies the digital signature of both image and configuration files.</td>
</tr>
<tr>
<td>Image</td>
<td>Verifies the digital signature of image files only.</td>
</tr>
<tr>
<td>None</td>
<td>Disables digital signature verification for both images and configuration files.</td>
</tr>
<tr>
<td>Script</td>
<td>Verifies the digital signature of configuration files.</td>
</tr>
</tbody>
</table>

3.7.35 no file verify
Resets the configured digital signature verification value to the factory default value.

Format: no file verify
Mode: Global Config

3.7.36 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. Use the confirm keyword to directly save the configuration to NVRAM without prompting for a confirmation.

Format: write memory [confirm]
Mode: Priviledged EXEC
3.8 SFP handling Commands
A new SFP handling is implemented. The SFP present state is periodically polled and if changed the SFP is enabled or disabled. If the SFP present state has changed a SNMP trap (and logging message) is generated.

The feature SFP auto-isolate disables a SFP port as long as no SFP is present.

The feature SFP auto-config reads the ethernet compliance in the EEPROM. If existing and applicable the SFP is configured related to the Ethernet protocol and then enabled, otherwise the SFP keeps disabled. Both features can be overridden and the SFP is then enabled even it is not present (auto-isolate) or the mode is not applicable (auto-config).

3.8.1 sfp auto-isolate
This command enables the feature auto-isolate.

Default: enabled
Format: sfp auto-isolate
Mode: Interface Config

3.8.1.1 no sfp auto-isolate
This command disables the feature auto-isolate. If the feature is disabled a port is enabled although no SFP is present.

Format: no sfp auto-isolate
Mode: Interface Config

3.8.2 sfp auto-configure
This command enables the feature auto-configure.

Default: enabled
Format: sfp auto-configure
Mode: Interface Config

3.8.2.1 no sfp auto-configure
This command disables the feature auto-configure. If the feature is disabled a port is enabled although the ethernet compliance mode is not applicable.

Format: no sfp auto-configure
Mode: Interface Config
### 3.8.3 sfp protocol
This command overrides the ethernet protocol read from the EEPROM. If the specified mode is applicable, the SFP is configured with this mode and enabled.

**Format**

```
sfp protocol 1000BASE-CX
sfp protocol 1000BASE-LX
sfp protocol 1000BASE-SX
sfp protocol 1000BASE-T
sfp protocol 10GBASE-CR
sfp protocol 10GBASE-ER
sfp protocol 10GBASE-LR
sfp protocol 10GBASE-LR4
sfp protocol 10GBASE-SR
sfp protocol 40GBASE-CR4
sfp protocol 40GBASE-LR4
sfp protocol 40GBASE-SR4
```

**Mode**

Interface Config

### 3.8.3.1 no sfp protocol
This command disables the SFP.

**Format**

```
no sfp protocol
```

**Mode**

Interface Config

### 3.8.4 snmp-server enable traps sfp
This command enables the sending of a trap if the SFP present status has changed.

The command ‘snmp-server enable traps’ is a standard FASTPATH command, the parameter ‘sfp’ has been added by Kontron. The ‘show trapflags’ command is the standard FASTPATH command to show the trap settings, the SFP trap indication has been added by Kontron.

**Default**

enabled

**Format**

```
snmp-server enable traps sfp
```

**Mode**

Global Config

### 3.8.4.1 no snmp-server enable traps sfp
This command disables the sending of a trap if the SFP present status has changed.

The command ‘snmp-server enable traps’ is a standard FASTPATH command, the parameter ‘sfp’ has been added by Kontron. The ‘show trapflags’ command is the standard FASTPATH command to show the trap settings, the SFP trap indication has been added by Kontron.

**Format**

```
no snmp-server enable traps sfp
```

**Mode**

Global Config
3.8.5  show sfp
This command displays information for a specified or all existing SFP's. For 'detail' the EEPROM data are indicated, for all
other commands the SFP present status, port-status (if port is enabled or disabled) and link-status are indicated. For
specified SFP additionally 'loss-of-signal' and 'transmitter-fault' are indicated.
If feature auto-isolate is set, the status of the feature (enabled/disabled) is indicated.
If feature auto-configure is set, the status of the feature (enabled/disabled), transceiver ID and ethernet protocol are dis-
played.

Format  show sfp slot/port [detail]
show sfp all
Mode     Privileged EXEC

3.9  Commands to configure startup services
This feature activates support for listing and configuring startup services. Services are board specific and defined by the
BSP.
The commands invoke the /opt/kontron/bin/chkconfig utility directly.

3.9.1  set chkconfig
This command configures a BSP startup service.

Format  set chkconfig <service>
Mode     Privileged EXEC

3.9.1.1  no set chkconfig
This command disables a BSP startup service.

Format  no set chkconfig <service>
Mode     Privileged EXEC

Note that disabling basic services may make the system unusable, e.g. disabling syslogd or FASTPATH may make the sys-
tem inaccessible.

3.9.2  show chkconfig
This command displays all currently installed services. Services are board specific and defined by the BSP.

Format  show chkconfig
Mode     Privileged EXEC

3.10  Simple Network Time Protocol Commands
This section describes the commands you use to automatically configure the system time and date by using Simple Net-
work Time Protocol (SNTP).

3.10.1  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 10.

Default  6
Format    sntp broadcast client poll-interval poll-interval
Mode      Global Config
3.10.1.1 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

3.10.2 sntp client mode
This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.
Multicast: For multicast mode the SNTP multicast address must be defined as a route to a device. This is set automatically to the network device (if networkport is specified) or serviceport device (if serviceport is specified). If deleting multicast mode the route is automatically deleted too.

Default: disabled
Format: sntp client mode [broadcast | unicast | multicast]
Mode: Global Config

3.10.2.1 no sntp client mode
This command disables Simple Network Time Protocol (SNTP) client mode.

Format: no sntp client mode
Mode: Global Config

3.10.3 sntp client port
This command sets the SNTP client port ID to 0, 123 or a value between 1025 and 65535. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying OS.

Default: 0
Format: sntp client port portid
Mode: Global Config

3.10.3.1 no sntp client port
This command resets the SNTP client port back to its default value.

Format: no sntp client port
Mode: Global Config

3.10.4 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 10.

Default: 6
Format: sntp unicast client poll-interval poll-interval
Mode: Global Config
3.10.4.1 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

3.10.5 sntp multicast client poll-interval
This command will set the poll interval for SNTP multicast clients in seconds as a power of two where <poll-interval> can be a value from 6 to 10.

Default: 6
Format: sntp multicast client poll-interval <poll-interval>
Mode: Global Config

3.10.5.1 no sntp multicast client poll-interval
This command resets the poll interval for SNTP multicast clients to its default value.

Format: no sntp multicast client poll-interval
Mode: Global Config

3.10.6 sntp unicast client poll-timeout
This command sets the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

Default: 5
Format: snntp unicast client poll-timeout poll-timeout
Mode: Global Config

3.10.6.1 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

3.10.7 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
3.10.7.1 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

3.10.8 sntp server
This command configures an SNTP server (a maximum of three). The server address can be either an IPv4 address or an IPv6 address. 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 | ipv6address | hostname} [priority] [version] [portid]
Mode Global Config

3.10.8.1 no sntp server
This command deletes an server from the configured SNTP servers.

Format no sntp server remove {ipaddress | ipv6address | hostname}
Mode Global Config

3.10.9 sntp source-interface
Use this command to specify the physical or logical interface to use as the source interface (source IP address) for SNTP unicast server configuration. If configured, the address of source interface is used for all SNTP communications between the SNTP server and the SNTP client. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the SNTP client falls back to its default behavior.

Format sntp source-interface {slot/port | loopback loopback-id | vlan vlan-id}
Mode Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>The unit identifier assigned to the switch.</td>
</tr>
<tr>
<td>loopback-id</td>
<td>Configures the loopback interface. The range of the loopback ID is 0 to 7.</td>
</tr>
<tr>
<td>tunnel-id</td>
<td>Configures the IPv6 tunnel interface. The range of the tunnel ID is 0 to 7.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.</td>
</tr>
</tbody>
</table>
3.10.9.1  no sntp source-interface
Use this command to reset the SNTP source interface to the default settings.

**Format**

no sntp source-interface

**Mode**

Global Config

3.10.10  show sntp
This command is used to display SNTP settings and status.

**Format**

show sntp

**Mode**

Privileged EXEC

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

3.10.11  show sntp client
This command is used to display SNTP client settings.

**Format**

show sntp client

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Supported Modes</td>
<td>Supported SNTP Modes (Broadcast or Unicast).</td>
</tr>
<tr>
<td>SNTP Version</td>
<td>The highest SNTP version the client supports.</td>
</tr>
<tr>
<td>Port</td>
<td>SNTP Client Port. The field displays the value 0 if it is default value. When the client port value is 0, if the client is in broadcast mode, it binds to port 123; if the client is in unicast mode, it binds to the port assigned by the underlying OS.</td>
</tr>
<tr>
<td>Client Mode</td>
<td>Configured SNTP Client Mode.</td>
</tr>
</tbody>
</table>

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

**Format**

show sntp server

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Host Address</td>
<td>IP address or hostname of configured SNTP Server.</td>
</tr>
<tr>
<td>Server Type</td>
<td>Address type of server (IPv4, IPv6, or DNS).</td>
</tr>
<tr>
<td>Server Stratum</td>
<td>Claimed stratum of the server for the last received valid packet.</td>
</tr>
<tr>
<td>Server Reference ID</td>
<td>Reference clock identifier of the server for the last received valid packet.</td>
</tr>
</tbody>
</table>
### 3.10.13  show sntp source-interface

Use this command to display the SNTP client source interface configured on the switch.

**Format**

```
show sntp source-interface
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNTP Client Source Interface</td>
<td>The interface ID of the physical or logical interface configured as the SNTP client source interface.</td>
</tr>
<tr>
<td>SNTP Client Source IPv4 Address</td>
<td>The IP address of the interface configured as the SNTP client source interface.</td>
</tr>
</tbody>
</table>

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

(Routing) #show sntp source-interface

SNTP Client Source Interface............... (not configured)

(Routing) #

### 3.11  Time Zone Commands

Use the Time Zone commands to configure system time and date, Time Zone and Summer Time (that is, Daylight Saving Time). Summer time can be recurring or non-recurring.

#### 3.11.1  clock set

This command sets the system time and date.

**Format**

```
clock set hh:mm:ss
clock set mm/dd/yyyy
```

**Mode**

Global Config
Example: The following shows examples of the command.

(FASTPATH Routing) (Config)# clock set 03:17:00
(FASTPATH Routing) (Config)# clock set 11/01/2011

3.11.2 clock summer-time date

Use the clock summer-time date command to set the summer-time offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they are read as either 0 or \0, as appropriate.

Format: clock summer-time date {date month year hh:mm:ss date month year hh:mm:ss} [offset offset] [zone acronym]

Mode: Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>Day of the month. Range is 1 to 31.</td>
</tr>
<tr>
<td>month</td>
<td>Month. Range is the first three letters by name; jan, for example.</td>
</tr>
<tr>
<td>year</td>
<td>Year. The range is 2000 to 2097.</td>
</tr>
<tr>
<td>hh:mm</td>
<td>Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.</td>
</tr>
<tr>
<td>offset</td>
<td>The number of minutes to add during the summertime. The range is 1 to 1440.</td>
</tr>
<tr>
<td>acronym</td>
<td>The acronym for the summer-time to be displayed when summertime is in effect. The range is up to four characters are allowed.</td>
</tr>
</tbody>
</table>

Example: The following shows examples of the command.

(FASTPATH Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
(FASTPATH Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18 offset 120 zone INDA

3.11.3 clock summer-time recurring

This command sets the summer-time recurring parameters.

Format: clock summer-time recurring {week day month hh:mm week day month hh:mm} [offset offset] [zone acronym]

Mode: Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
<td>The system clock uses the standard recurring summer time settings used in countries in the European Union.</td>
</tr>
<tr>
<td>USA</td>
<td>The system clock uses the standard recurring daylight saving time settings used in the United States.</td>
</tr>
<tr>
<td>week</td>
<td>Week of the month. The range is 1 to 5, first, last.)</td>
</tr>
<tr>
<td>day</td>
<td>Day of the week. The range is the first three letters by name; sun, for example.</td>
</tr>
<tr>
<td>month</td>
<td>Month. The range is the first three letters by name; jan, for example.</td>
</tr>
</tbody>
</table>
Example: The following shows examples of the command.

```
(FASTPATH Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18
(FASTPATH Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18 offset 120 zone INDA
```

3.11.3.1 no clock summer-time

This command disables the summer-time settings.

<table>
<thead>
<tr>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>no clock summer-time</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

Example: The following shows an example of the command.

```
(FASTPATH Routing) (Config)# no clock summer-time
```

3.11.4 clock timezone

Use this command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either 0 or \0 as appropriate.

<table>
<thead>
<tr>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock timezone (hours) [minutes minutes] [zone acronym]</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

Example: The following shows an example of the command.

```
(FASTPATH Routing) (Config)# clock timezone 5 minutes 30 zone INDA
```
3.11.4.1 no clock timezone
Use this command to reset the time zone settings.

**Format**

no clock timezone

**Mode**

Global Config

**Example:** The following shows an example of the command.

(FASTPATH Routing) (Config)# no clock timezone

3.11.5 show clock
Use this command to display the time and date from the system clock.

**Format**

show clock

**Mode**

Privileged EXEC

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

(FASTPATH Routing) # show clock
15:02:09 (UTC+0:00) Nov 1 2011
No time source

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

With the above configuration the output appears as below:

(FASTPATH Routing) # show clock
10:55:40 INDA(UTC+7:30) Nov 1 2011
No time source

3.11.6 show clock detail
Use this command to display the detailed system time along with the time zone and the summertime configuration.

**Format**

show clock detail

**Mode**

Privileged EXEC

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

(FASTPATH Routing) # show clock detail
15:05:24 (UTC+0:00) Nov 1 2011
No time source

Time zone:
Acronym not configured
Offset is UTC+0:00

Summertime:
Summer-time is disabled

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

With the above configuration the output appears as below:

(FASTPATH Routing) # show clock detail
10:57:57 INDA(UTC+7:30) Nov 1 2011
No time source
Time zone:
Acronym is INDA
Offset is UTC+5:30

Summertime:
Acronym is INDA
Recurring every year
Begins on second Sunday of Nov at 03:18
Ends on second Monday of Nov at 03:18
Offset is 120 minutes
Summer-time is in effect.

3.12 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.

3.12.1 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

3.12.1.1 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

3.12.2 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
3.12.2.1 no client-identifier
This command deletes the client identifier.

_format_  no client-identifier
_mode_  DHCP Pool Config

3.12.3 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

3.12.3.1 no client-name
This command removes the client name.

_format_  no client-name
_mode_  DHCP Pool Config

3.12.4 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

3.12.4.1 no default-router
This command removes the default router list.

_format_  no default-router
_mode_  DHCP Pool Config

3.12.5 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
3.12.5.1 no dns-server
This command removes the DNS Server list.

**Format**
no dns-server

**Mode**
DHCP Pool Config

3.12.6 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

3.12.6.1 no hardware-address
This command removes the hardware address of the DHCP client.

**Format**
no hardware-address

**Mode**
DHCP Pool Config

3.12.7 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

3.12.7.1 no host
This command removes the IP address of the DHCP client.

**Format**
no host

**Mode**
DHCP Pool Config

3.12.8 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
3.12.8.1 no lease
This command restores the default value of the lease time for DHCP Server.

Format no lease
Mode DHCP Pool Config

3.12.9 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

3.12.9.1 no network
This command removes the subnet number and mask.

Format no network
Mode DHCP Pool Config

3.12.10 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

3.12.10.1 no bootfile
This command deletes the boot image name.

Format no bootfile
Mode DHCP Pool Config

3.12.11 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
3.12.11.1  **no domain-name**  
This command removes the domain name.

**Format**  
no domain-name

**Mode**  
DHCP Pool Config

3.12.12  **domain-name enable**  
This command enables the domain name functionality in FASTPATH.

**Format**  
domain-name enable [name name]

**Mode**  
Global Config

**Example:** The following shows an example of the command.

```
(Switching) (Config)#domain-name enable
(Switching) (Config)#exit
```

3.12.12.1  **no domain-name enable**  
This command disables the domain name functionality in FASTPATH.

**Format**  
no domain-name enable

**Mode**  
Global Config

3.12.13  **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**  
one

**Format**  
netbios-name-server address [address2...address8]

**Mode**  
DHCP Pool Config
3.12.13.1  no netbios-name-server
This command removes the NetBIOS name server list.

Format   no netbios-name-server
Mode     DHCP Pool Config

3.12.14  netbios-node-type
The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. 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

3.12.14.1  no netbios-node-type
This command removes the NetBIOS node Type.

Format   no netbios-node-type
Mode     DHCP Pool Config

3.12.15  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

3.12.15.1  no next-server
This command removes the boot server list.

Format   no next-server
Mode     DHCP Pool Config
3.12.16 option
The `option` command configures DHCP Server options. The `code` parameter specifies the DHCP option code and ranges from 1-254. The `ascii` 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).

<table>
<thead>
<tr>
<th>Default</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>`option code {ascii string</td>
</tr>
<tr>
<td>Mode</td>
<td>DHCP Pool Config</td>
</tr>
</tbody>
</table>

3.12.16.1 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 |

3.12.17 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 |

3.12.17.1 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 |

3.12.18 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 |
3.12.18.1  no ip dhcp ping packets
This command restores the number of ping packets to the default value.

Format   no ip dhcp ping packets
Mode     Global Config

3.12.19  service dhcp
This command enables the DHCP server.

Default  disabled
Format    service dhcp
Mode      Global Config

3.12.19.1  no service dhcp
This command disables the DHCP server.

Format    no service dhcp
Mode      Global Config

3.12.20  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

3.12.20.1  no ip dhcp bootp automatic
This command disables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

Format    no ip dhcp bootp automatic
Mode      Global Config

3.12.21  ip dhcp conflict logging
This command enables conflict logging on DHCP server.

Default  enabled
Format    ip dhcp conflict logging
Mode      Global Config
3.12.21.1 no ip dhcp conflict logging
This command disables conflict logging on DHCP server.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip dhcp conflict logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

3.12.22 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             |

3.12.23 clear ip dhcp server statistics
This command clears DHCP server statistics counters.

<table>
<thead>
<tr>
<th>Format</th>
<th>clear ip dhcp server statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.12.24 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.

<table>
<thead>
<tr>
<th>Default</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>clear ip dhcp conflict {address</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.12.25 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.

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip dhcp binding [address]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modes</td>
<td>• Privileged EXEC</td>
</tr>
<tr>
<td></td>
<td>• User EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IP address of the client.</td>
</tr>
<tr>
<td>Hardware Address</td>
<td>The MAC Address or the client identifier.</td>
</tr>
<tr>
<td>Lease expiration</td>
<td>The lease expiration time of the IP address assigned to the client.</td>
</tr>
<tr>
<td>Type</td>
<td>The manner in which IP address was assigned to the client.</td>
</tr>
</tbody>
</table>
3.12.26 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service DHCP</td>
<td>The field to display the status of dhcp protocol.</td>
</tr>
<tr>
<td>Number of Ping Packets</td>
<td>The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.</td>
</tr>
<tr>
<td>Conflict Logging</td>
<td>Shows whether conflict logging is enabled or disabled.</td>
</tr>
<tr>
<td>BootP Automatic</td>
<td>Shows whether BootP for dynamic pools is enabled or disabled.</td>
</tr>
</tbody>
</table>

3.12.27 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool Name</td>
<td>The name of the configured pool.</td>
</tr>
<tr>
<td>Pool Type</td>
<td>The pool type.</td>
</tr>
<tr>
<td>Lease Time</td>
<td>The lease expiration time of the IP address assigned to the client.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>The list of DNS servers available to the DHCP client.</td>
</tr>
<tr>
<td>Default Routers</td>
<td>The list of the default routers available to the DHCP client.</td>
</tr>
</tbody>
</table>

The following additional field is displayed for Dynamic pool type:

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>The network number and the mask for the DHCP address pool.</td>
</tr>
</tbody>
</table>

The following additional fields are displayed for Manual pool type:

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name</td>
<td>The name of a DHCP client.</td>
</tr>
<tr>
<td>Client Identifier</td>
<td>The unique identifier of a DHCP client.</td>
</tr>
<tr>
<td>Hardware Address</td>
<td>The hardware address of a DHCP client.</td>
</tr>
<tr>
<td>Hardware Address Type</td>
<td>The protocol of the hardware platform.</td>
</tr>
<tr>
<td>Host</td>
<td>The IP address and the mask for a manual binding to a DHCP client.</td>
</tr>
</tbody>
</table>
3.12.28  show ip dhcp server statistics

This command displays DHCP server statistics.

**Format**

```plaintext
show ip dhcp server statistics
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Bindings</td>
<td>The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.</td>
</tr>
<tr>
<td>Expired Bindings</td>
<td>The number of expired leases.</td>
</tr>
<tr>
<td>Malformed Bindings</td>
<td>The number of truncated or corrupted messages that were received by the DHCP server.</td>
</tr>
</tbody>
</table>

**Message Received:**

<table>
<thead>
<tr>
<th>Message</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP DISCOVER</td>
<td>The number of DHCPDISCOVER messages the server has received.</td>
</tr>
<tr>
<td>DHCP REQUEST</td>
<td>The number of DHCPREQUEST messages the server has received.</td>
</tr>
<tr>
<td>DHCP DECLINE</td>
<td>The number of DHCPDECLINE messages the server has received.</td>
</tr>
<tr>
<td>DHCP RELEASE</td>
<td>The number of DHCPRELEASE messages the server has received.</td>
</tr>
<tr>
<td>DHCP INFORM</td>
<td>The number of DHCPINFORM messages the server has received.</td>
</tr>
</tbody>
</table>

**Message Sent:**

<table>
<thead>
<tr>
<th>Message</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP OFFER</td>
<td>The number of DHCPOFFER messages the server sent.</td>
</tr>
<tr>
<td>DHCP ACK</td>
<td>The number of DHCPACK messages the server sent.</td>
</tr>
<tr>
<td>DHCP NACK</td>
<td>The number of DHCPNACK messages the server sent.</td>
</tr>
</tbody>
</table>

3.12.29  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**

```plaintext
show ip dhcp conflict [ip-address]
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IP address of the host as recorded on the DHCP server.</td>
</tr>
<tr>
<td>Detection Method</td>
<td>The manner in which the IP address of the hosts were found on the DHCP Server.</td>
</tr>
<tr>
<td>Detection time</td>
<td>The time when the conflict was found.</td>
</tr>
</tbody>
</table>
3.12.30  ip dhcp option-61
This command specifies the mode for setting a DHCP client identifier (DHCP option 61). The client identifier is sent if one of the options below is specified, otherwise (default, “no”-command) the option is disabled. The user can either select an automatic constructed unique ID (“auto”/“variant-1” or “oem”) or define a fixed string which should be unique too (“fixed”).

If a fixed string is defined, the identifier is preceded by a byte 0x00 which defines the hardware-type (other).

The automatic identifier is constructed as:
- “auto”:
  a byte 0x00 (hardware type) followed by a ascii string containing the MAC Address and the network management VLAN ID separated by “-vl” (e.g. 0x00 "00a0.a573.449c-vl1")
- “variant-1”/“oem”:
  byte 1: 0x00 (hardware type)
  bytes 2-5: shelf address information (cabinet row/column and chassis vertical/horizontal dev)
  bytes 6-8: address information (logical slot number, module type and number)
  bytes 9-10: shelf address information (cabinet and subrack HMS number)
  byte 11-12: device ID
  byte 13: request identifier (=0xff)
  bytes 14-16: release information (version/edition/repair)

Format  ip dhcp option-61 <string>
         ip dhcp option-61 auto
         ip dhcp option-61 oem

Modes  Global Config

3.12.30.1  no ip dhcp option-61
This command disables DHCP client identifier (DHCP option 61).

Format  no ip dhcp option-61

Modes  Global Config

3.12.31  show ip dhcp option-61
This command shows the configured type of the client identifier or (if none) disabled. If the feature is enabled the specified (“fixed”) or the automatic client-identifier is shown additionally.

Format  show ip dhcp option-61

Modes  Privileged Exec

3.13  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.

3.13.1  ip domain lookup
Use this command to enable the DNS client.

Default  enabled
Format  ip domain lookup
Mode    Global Config
3.13.1   **no ip domain lookup**

Use this command to disable the DNS client.

**Format**  
no ip domain lookup

**Mode**  
Global Config

3.13.2   **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.

3.13.2.1   **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

3.13.3   **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

3.13.3.1   **no ip domain list**

Use this command to delete a name from a list.

**Format**  
no ip domain list name

**Mode**  
Global Config
3.13.4  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 IPv4 or IPv6 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

3.13.4.1  no ip name server

Use this command to remove a name server.

**Format**

```
no ip name-server [server-address1...server-address8]
```

**Mode**

Global Config

3.13.5  ip name source-interface

Use this command to specify the physical or logical interface to use as the DNS client (IP name) source interface (source IP address) for the DNS client management application. If configured, the address of source Interface is used for all DNS communications between the DNS server and the DNS client. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (out-bound) interface is used as the source address. If the configured interface is down, the DNS client falls back to its default behavior.

**Format**

```
ip name-source-interface {slot/port | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}
```

**Mode**

Global Config

3.13.5.1  no ip name source-interface

Use this command to reset the DNS source interface to the default settings.

**Format**

```
no ip name-source-interface
```

**Mode**

Global Config

3.13.6  ip host

Use this command to define static host name-to-address mapping in the host cache. The parameter *name* is host name and *ip address* is the IP address of the host. The hostname can include 1–255 alphanumeric characters, periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example "lab-pc 45".

**Default**

none

**Format**

```
ip host name ipaddress
```

**Mode**

Global Config
3.13.6.1  no ip host
Use this command to remove the name-to-address mapping.

Format  no ip host name
Mode    Global Config

3.13.7  ipv6 host
Use this command to define static host name-to-IPv6 address mapping in the host cache. The parameter name is host name and v6 address is the IPv6 address of the host. The hostname can include 1–255 alphanumeric characters, periods, hyphens, and spaces. Hostnames that include one or more spaces must be enclosed in quotation marks, for example "lab-pc 45".

Default  none
Format    ipv6 host name v6 address
Mode      Global Config

3.13.7.1  no ipv6 host
Use this command to remove the static host name-to-IPv6 address mapping in the host cache.

Format  no ipv6 host name
Mode    Global Config

3.13.8  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

3.13.8.1  no ip domain retry
Use this command to return to the default.

Format  no ip domain retry number
Mode    Global Config

3.13.9  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. The parameter seconds ranges from 0 to 3600.

Default  3
Format    ip domain timeout seconds
Mode      Global Config
3.13.9.1 no ip domain timeout
Use this command to return to the default setting.

Format no ip domain timeout seconds
Mode Global Config

3.13.10 clear host
Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format clear host {name | all}
Mode Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>A particular host entry to remove. The parameter name ranges from 1-255 characters.</td>
</tr>
<tr>
<td>all</td>
<td>Removes all entries.</td>
</tr>
</tbody>
</table>

3.13.11 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. The parameter name ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

Format show hosts [name]
Mode Privileged EXEC
User EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Domain host name.</td>
</tr>
<tr>
<td>Default Domain</td>
<td>Default domain name.</td>
</tr>
<tr>
<td>Default Domain List</td>
<td>Default domain list.</td>
</tr>
<tr>
<td>Domain Name Lookup</td>
<td>DNS client enabled/disabled.</td>
</tr>
<tr>
<td>Number of Retries</td>
<td>Number of time to retry sending Domain Name System (DNS) queries.</td>
</tr>
<tr>
<td>Retry Timeout Period</td>
<td>Amount of time to wait for a response to a DNS query.</td>
</tr>
<tr>
<td>Name Servers</td>
<td>Configured name servers.</td>
</tr>
<tr>
<td>DNS Client Source Interface</td>
<td>Shows the configured source interface (source IP address) used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the command.
<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
DNS Client Source Interface....... (not configured)

Configured host name-to-address mapping:

<table>
<thead>
<tr>
<th>Host</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting.gm.com</td>
<td>176.16.8.8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Host</th>
<th>Total</th>
<th>Elapsed</th>
<th>Type</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.stanford.edu">www.stanford.edu</a></td>
<td>72</td>
<td>3</td>
<td>IP</td>
<td>171.64.14.203</td>
</tr>
</tbody>
</table>

3.13.12 show ip name source-interface

Use this command to display the configured source interface details used for a DNS client. The IP address of the selected interface is used as source IP for all communications with the server.

Format show ip name source-interface

Mode Privileged EXEC

3.14 IP Address Conflict Commands

The commands in this section help troubleshoot IP address conflicts.

3.14.1 ip address-conflict-detect run

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format ip address-conflict-detect run

Mode
  • Global Config
  • Virtual Router Config

3.14.2 show ip address-conflict

This command displays the status information corresponding to the last detected address conflict.

Format show ip address-conflict

Modes Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Conflict Detection Status</td>
<td>Identifies whether the switch has detected an address conflict on any IP address.</td>
</tr>
<tr>
<td>Last Conflicting IP Address</td>
<td>The IP Address that was last detected as conflicting on any interface.</td>
</tr>
<tr>
<td>Last Conflicting MAC Address</td>
<td>The MAC Address of the conflicting host that was last detected on any interface.</td>
</tr>
<tr>
<td>Time Since Conflict Detected</td>
<td>The time in days, hours, minutes and seconds since the last address conflict was detected.</td>
</tr>
</tbody>
</table>
3.14.3 clear ip address-conflict-detect
This command clears the detected address conflict status information.

Format: clear ip address-conflict-detect
Modes: Privileged EXEC

3.15 Serviceability Packet Tracing Commands
These commands improve the capability of network engineers to diagnose conditions affecting their FASTPATH product. Remember to upload the existing fastpath.cfg file off the switch prior to loading a new release image in order to make a backup.

The output of “debug” commands can be long and may adversely affect system performance.

3.15.1 capture start
Use the command capture start to manually start capturing CPU packets for packet trace.
The packet capture operates in three modes:
• capture file
• remote capture
• capture line
The command is not persistent across a reboot cycle.

Format: capture start [{all|receive|transmit}]
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Capture all traffic.</td>
</tr>
<tr>
<td>receive</td>
<td>Capture only received traffic.</td>
</tr>
<tr>
<td>transmit</td>
<td>Capture only transmitted traffic.</td>
</tr>
</tbody>
</table>

3.15.2 capture stop
Use the command capture stop to manually stop capturing CPU packets for packet trace.

Format: capture stop
Mode: Privileged EXEC

3.15.3 capture file|remote|line
Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format: capture {file|remote|line}
Mode: Global Config
3.15.4 capture remote port

Use this command to configure file capture options. The command is persistent across a reboot cycle. The id parameter is a TCP port number from 1024–49151.

Format: `capture remote port id`

Mode: Global Config

3.15.5 capture file size

Use this command to configure file capture options. The command is persistent across a reboot cycle. The max-file-size parameter is the maximum size the pcap file can reach, which is 2–512 KB.

Format: `capture file size max file size`

Mode: Global Config

3.15.6 capture line wrap

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity.

Format: `capture line wrap`

Mode: Global Config
3.15.6.1 no capture line wrap
This command disables wrapping of captured packets and configures capture packet to stop when the captured packet capacity is full.

Format  no capture line wrap
Mode    Global Config

3.15.7 show capture packets
Use this command to display packets captured and saved to RAM. It is possible to capture and save into RAM, packets that are received or transmitted through the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.
Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Format  show capture packets
Mode    Privileged EXEC

3.15.8 cpu-traffic direction interface
Use this command to associate CPU filters to an interface or list of interfaces. The interfaces can be a physical or logical LAG. The statistics counters are updated only for the configured interfaces. The traces can also be obtained for the configured interfaces.

The offset should consider the VLAN tag headers as the packet to the CPU is always a tagged packet.

Default None
Format  cpu-traffic direction {tx|rx|both} interface interface-range
Mode    Global Config

3.15.8.1 no cpu-traffic direction interface
Use this command to remove all interfaces from the CPU filters.

Format  no cpu-traffic direction {tx|rx|both} interface interface-range
Mode    Global Config
3.15.9  cpu-traffic direction match cust-filter

Use this command to configure a custom filter. The statistics and/or traces for configured filters are obtained for the packet matching configured data at the specific offset. If the mask is not specified then the default mask is 0xFF. There can be three different offsets specified as match conditions. Each time a custom filter is configured, the switch overrides the previous configuration.

The offset should consider the VLAN tag headers as the packet to the CPU is always a tagged packet.

Default: None

Format:
```
cpu-traffic direction {tx|rx|both} match cust-filter offset1 data1 [mask1 mask1]
offset2 data2 [mask2 mask2] offset3 data3 [mask3 mask3]
```

Mode: Global Config

3.15.9.1  no cpu-traffic direction match cust-filter

Use this command to remove the configured custom filter.

Format:
```
no cpu-traffic direction {tx|rx|both} match cust-filter offset1 data1 [mask1 mask1]
offset2 data2 [mask2 mask2] offset3 data3 [mask3 mask3]
```

Mode: Global Config

3.15.10  cpu-traffic direction match srcip

Use this command to configure the source IP address-specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured source IP/Mask.

Default: None

Format:
```
cpu-traffic direction {tx|rx|both} match srcip ipaddress [mask mask]
```

Mode: Global Config

3.15.10.1  no cpu-traffic direction match srcip

Use this command to disable the configured source IP address filter.

Format:
```
no cpu-traffic direction {tx|rx|both} match srcip ipaddress [mask mask]
```

Mode: Global Config

3.15.11  cpu-traffic direction match dstip

Use this command to configure the destination IP address-specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured destination IP/Mask.

Default: None

Format:
```
cpu-traffic direction {tx|rx|both} match dstip ipaddress [mask mask]
```

Mode: Global Config
3.15.11.1  no cpu-traffic direction match dstip
Use this command to disable the configured destination IP address filter.

Format  
         no cpu-traffic direction {tx|rx|both} match dstip ipaddress [mask mask]
Mode    
         Global Config

3.15.12  cpu-traffic direction match tcp
Use this command to configure the source or destination TCP port-specific filter. The statistics and/or traces for configured filters are obtained for the packet matching configured source/destination TCP port.

Default  
         None
Format  
         cpu-traffic direction {tx|rx|both} match {srctp|dstdtcp} port [mask mask]
Mode    
         Global Config

3.15.12.1  no cpu-traffic direction match tcp
Use this command to remove the configured source/destination TCP port filter.

Format  
         no cpu-traffic direction {tx|rx|both} match {srctp|dstdtcp} port [mask mask]
Mode    
         Global Config

3.15.13  cpu-traffic direction match udp
Use this command to configure the source or destination UDP port-specific filter. The statistics and/or traces for configured filters are obtained for the packet matching configured source/destination UDP port.

Default  
         None
Format  
         cpu-traffic direction {tx|rx|both} match {srctudp|dstdudp} port [mask mask]
Mode    
         Global Config

3.15.13.1  no cpu-traffic direction match udp
Use this command to remove the configured source/destination UDP port filter.

Format  
         no cpu-traffic direction {tx|rx|both} match {srctudp|dstdudp} port [mask mask]
Mode    
         Global Config

3.15.14  cpu-traffic mode
Use this command to configure CPU-traffic mode. The packets in the RX/TX direction are matched when the mode is enabled.

Default  
         Disabled
Format  
         cpu-traffic mode
Mode    
         Global Config
3.15.14.1  no cpu-traffic mode
Use this command to disable CPU-traffic mode.

Format          no cpu-traffic mode
Mode            Global Config

3.15.15    cpu-traffic trace
Use this command to configure CPU packet tracing. The packet can be received by multiple components. If the feature is enabled and tracing configured, the packets are traced per the defined filter. If dump-pkt is enabled, the first 64 bytes of the packet are displayed along with the trace statistics.

Default        Disabled
Format          cpu-traffic trace {dump-pkt}
Mode            Global Config

3.15.15.1  no cpu-traffic trace
Use this command to disable CPU packet tracing and dump-pkt (if configured).

Format          no cpu-traffic trace {dump-pkt}
Mode            Global Config

3.15.15.2    show cpu-traffic
Use this command to display the current configuration parameters.

Default        None
Format          show cpu-traffic
Mode            Privileged EXEC

Example:
(Routing) #show cpu-traffic

Admin Mode.............................. Disable
Packet Trace.............................. Disable
Packet Dump.............................. Disable

Direction TX:
Filter Options........................... N/A
Interface.................................. N/A
Src TCP parameters........................ 0 0
Dst TCP parameters........................ 0 0
Src UDP parameters........................ 0 0
Dst UDP parameters........................ 0 0
Src IP parameters........................ 0.0.0.0 0.0.0.0
Dst IP parameters........................ 0.0.0.0 0.0.0.0
Src MAC parameters........................ 00:00:00:00:00:00 00:00:00:00:00:00
Dst MAC parameters........................ 00:00:00:00:00:00 00:00:00:00:00:00
Custom filter parameters1................ Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters2................ Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters3................ Offset=0x0 Value=0x0 Mask=0x0

Direction RX:
Filter Options........................... N/A
Interface.................................. N/A
Src TCP parameters......................... 0 0
Dst TCP parameters......................... 0 0
Src UDP parameters......................... 0 0
Dst UDP parameters......................... 0 0
Src IP parameters........................ 0.0.0.0 0.0.0.0
Dst IP parameters........................ 0.0.0.0 0.0.0.0
Src MAC parameters......................... 00:00:00:00:00:00 00:00:00:00:00:00
Dst MAC parameters......................... 00:00:00:00:00:00 00:00:00:00:00:00
Custom filter parameters1................. Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters2................. Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters3................. Offset=0x0 Value=0x0 Mask=0x0

3.15.16 show cpu-traffic interface

Use this command to display per interface statistics for configured filters. The statistics can be displayed for a specific filter (e.g., stp, udld, arp etc). If no filter is specified, statistics are displayed for all configured filters. Similarly, source/destination IP, TCP, UDP or MAC along with custom filter can be used as command option to get statistics.

Default None
Format show cpu-traffic interface {all | unit/slot/port | cpu } filter
Mode Privileged EXEC

3.15.17 show cpu-traffic summary

Use this command to display summary statistics for configured filters for all interfaces.

Default None
Format show cpu-traffic summary
Mode Privileged EXEC

Example:
(Routing) #show cpu-traffic summary

<table>
<thead>
<tr>
<th>Filter</th>
<th>Received</th>
<th>Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LACPDU</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ARP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>UDLD</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LLDP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OSPF</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BGP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DHCP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BCAST</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MCAST</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>UCAST</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SRCIP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DSTIP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SRCMAC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DSTMAC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CUSTOM</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SRCTCP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DSTTCP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SRCUDP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
3.15.18 show cpu-traffic trace

Use this command to display traced information. The trace information can be displayed either for all available packets or for specific filter (e.g., stp, udld, arp etc). Similarly, source/destination IP or MAC along with custom filter can be used as command option to get specific traces from history. If enabled, packet dump information is displayed along with packet trace statistics. By default, packet dump buffer size is set to store first 64 bytes of packet.

Default: None
Format: show cpu-traffic trace filter
Mode: Privileged EXEC

Example:
(Routing) #show cpu-traffic summary
Packet #1: IP; DHCP; UCAST; SRCMAC=00:10:10:10:10:10;
<08:06:10> Sysnet received in sysNetNotifyPduReceive()
<08:06:10> Packet delivered to IP via ipMapRecvIP()
<08:06:10> Freed
0000 00 10 10 18 82 18 b3 00 10 10 10 10 10 81 00 00 01 ............
0010 08 00 45 10 01 21 00 00 00 00 40 11 79 bd 00 00 ..E..!....@.y...
0020 00 00 ff ff ff ff ff 00 44 00 43 01 0d 48 10 03 01 ...D.C..H...
0030 06 00 18 85 4a 83 00 00 80 00 00 00 00 00 00 00 00 ...........J

3.15.19 clear cpu-traffic

Use this command to clear cpu-traffic statistics or trace information on all interfaces.

Default: None
Format: clear cpu-traffic {counters | traces}
Mode: Global Config

3.15.20 debug aaa accounting

This command is useful to debug accounting configuration and functionality in User Manager.

Format: debug aaa accounting
Mode: Privileged EXEC

3.15.20.1 no debug aaa accounting

Use this command to turn off debugging of User Manager accounting functionality.

Format: no debug aaa accounting
Mode: Privileged EXEC

3.15.21 debug aaa authorization

Use this command to enable the tracing for AAA in User Manager. This is useful to debug authorization configuration and functionality in the User Manager. Each of the parameters are used to configure authorization debug flags.

Format: debug aaa authorization commands|exec
Mode: Privileged EXEC
3.15.21 no debug aaa authorization
Use this command to turn off debugging of the User Manager authorization functionality.

**Format**
no debug aaa authorization

**Mode**
Privileged EXEC

**Example:** The following is an example of the command.

(Switching) #debug aaa authorization
Tacacs authorization receive packet tracing enabled.

(Switching) #debug tacacs authorization packet transmit
authorization tracing enabled.

(Switching) #no debug aaa authorization
AAA authorization tracing enabled

(Switching) #

3.15.22 debug arp
Use this command to enable ARP debug protocol messages.

**Default**
disabled

**Format**
debug arp

**Mode**
Privileged EXEC

3.15.22.1 no debug arp
Use this command to disable ARP debug protocol messages.

**Format**
no debug arp

**Mode**
Privileged EXEC

3.15.23 debug authentication
This command displays either the debug trace for either a single event or all events for an interface.

**Default**
none

**Format**
debug authentication packet {all | event} interface

**Mode**
Privileged EXEC

3.15.24 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|oui]

**Mode**
Privileged EXEC
3.15.24.1 no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format: no debug auto-voip
Mode: Privileged EXEC

3.15.25 debug clear

This command disables all previously enabled "debug" traces.

Default: disabled
Format: debug clear
Mode: Privileged EXEC

3.15.26 debug console

This command enables the display of "debug" trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default: disabled
Format: debug console
Mode: Privileged EXEC

3.15.26.1 no debug console

This command disables the display of "debug" trace output on the login session in which it is executed.

Format: no debug console
Mode: Privileged EXEC

3.15.27 debug crashlog

Use this command to view information contained in the crash log file that the system maintains when it experiences an unexpected reset. The crash log file contains the following information:

• Call stack information in both primitive and verbose forms
• Log Status
• Buffered logging
• Event logging
• Persistent logging
• System Information (output of sysapiMbufDump)
• Message Queue Debug Information
• Memory Debug Information
• Memory Debug Status
• OS Information (output of osapiShowTasks)
• /proc information (meminfo, cpuinfo, interrupts, version and net/sockstat)

Default: disabled
Format: debug crashlog [[kernel] crashlog-number [upload url] | proc | verbose | deleteall]
Mode: Privileged EXEC
### 3.15.28 debug dcbx packet

Use this command to enable debug tracing for DCBX packets that are transmitted or received.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kernel</td>
<td>View the crash log file for the kernel.</td>
</tr>
</tbody>
</table>
| crashlog-number  | Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4.  
                      deb                                                                 |
| upload url       | To upload the crash log (or crash dump) to a TFTP server, use the upload keyword and specify the required TFTP server information. |
| proc             | View the application process crashlog.                                     |
| verbose          | Enable the verbose crashlog.                                              |
| deleteall        | Delete all crash log files on the system.                                 |
| data             | Crash log data recorder.                                                   |
| crashdump-number | Specifies the crash dump number to view. The valid range is 0–2.           |
| download url     | To download a crash dump to the switch, use the download keyword and specify the required TFTP server information. |
| component-id     | The ID of the component that caused the crash.                            |
| item-number      | The item number.                                                           |
| additional-parameter | Additional parameters to include.                                       |

**Default**: disabled

**Format**: debug dcbx packet {receive | transmit}

**Mode**: Privileged EXEC

### 3.15.29 debug debug-config

Use this command to download or upload the debug-config.ini file. The debug-config.ini file executes CLI commands (including devshell and drivshell commands) on specific predefined events. The debug config file is created manually and downloaded to the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proc</td>
<td>View the application process crashlog.</td>
</tr>
<tr>
<td>verbose</td>
<td>Enable the verbose crashlog.</td>
</tr>
<tr>
<td>deleteall</td>
<td>Delete all crash log files on the system.</td>
</tr>
<tr>
<td>data</td>
<td>Crash log data recorder.</td>
</tr>
<tr>
<td>crashdump-number</td>
<td>Specifies the crash dump number to view. The valid range is 0–2.</td>
</tr>
<tr>
<td>download url</td>
<td>To download a crash dump to the switch, use the download keyword and specify the required TFTP server information.</td>
</tr>
</tbody>
</table>

**Default**: disabled

**Format**: debug debug-config {download <url> | upload <url>}

**Mode**: Privileged EXEC

### 3.15.30 debug dhcp packet

This command displays "debug" information about DHCPv4 client activities and traces DHCPv4 packets to and from the local DHCPv4 client.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kernel</td>
<td>View the crash log file for the kernel.</td>
</tr>
</tbody>
</table>
| crashlog-number  | Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4.  
                      deb                                                                 |
| upload url       | To upload the crash log (or crash dump) to a TFTP server, use the upload keyword and specify the required TFTP server information. |
| proc             | View the application process crashlog.                                     |
| verbose          | Enable the verbose crashlog.                                              |
| deleteall        | Delete all crash log files on the system.                                 |
| data             | Crash log data recorder.                                                   |
| crashdump-number | Specifies the crash dump number to view. The valid range is 0–2.           |
| download url     | To download a crash dump to the switch, use the download keyword and specify the required TFTP server information. |
| component-id     | The ID of the component that caused the crash.                            |
| item-number      | The item number.                                                           |
| additional-parameter | Additional parameters to include.                                       |

**Default**: disabled

**Format**: debug dhcp packet [transmit | receive]

**Mode**: Privileged EXEC
3.15.30.1 no debug dhcp
This command disables the display of "debug" trace output for DHCPv4 client activity.

Format no debug dhcp packet [transmit | receive]
Mode Privileged EXEC

3.15.31 debug dot1ag
Use this command to enable debugging of the messages sent between MPs and MEPs.

Default disabled
Format debug dot1ag {all | ccm | events | lbr | ltm | ltr | pdu}
Mode Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Debug all dot1ag message types.</td>
</tr>
<tr>
<td>CCM</td>
<td>Configure debug flags for Continuity Check Message information. A multicast CFM PDU transmitted periodically by a MEP in order to ensure continuity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to receiving a CCM.</td>
</tr>
<tr>
<td>LTM</td>
<td>Configure debug flags for Linktrace Message information. A CFM PDU initiated by a MEP to trace a path to a target MAC address, forwarded from MIP to MIP, up to the point at which the LTM reaches its target, a MEP, or can no longer be forwarded. Each MP along the path to the target generates an LTR.</td>
</tr>
<tr>
<td>LTR</td>
<td>Configure debug flags for Linktrace Reply information. A unicast CFM PDU sent by an MP to a MEP, in response to receiving an LTM from that MEP.</td>
</tr>
<tr>
<td>LBM</td>
<td>Configure debug flags for Loopback Message information. A unicast CFM PDU transmitted by a MEP, addressed to a specific MP, in the expectation of receiving an LBR.</td>
</tr>
<tr>
<td>LBR</td>
<td>Configure debug flags for Loopback Reply information. A unicast CFM PDU transmitted by an MP to a MEP, in response to an LBM received from that MEP.</td>
</tr>
<tr>
<td>PDU</td>
<td>Configure debug flags for CFM PDU information.</td>
</tr>
</tbody>
</table>

3.15.32 debug dot1x packet
Use this command to enable dot1x packet debug trace.

Default disabled
Format debug dot1x
Mode Privileged EXEC

3.15.32.1 no debug dot1x packet
Use this command to disable dot1x packet debug trace.

Format no debug dot1x
Mode Privileged EXEC
3.15.33 debug fip-snooping packet

Use the `debug fip-snooping packet` command in Privileged EXEC mode to enable FIP packet debug trace on transmit or receive path with different filter options configured.

**Default** disabled

**Format**
```
debug fip-snooping packet [{transmit | receive | filter {dst-mac mac-addr | fip,proto-code 1-15 | src-intf slot/port | src-mac mac-addr | vlan 1-4093}]
```

**Mode**
- User EXEC
- Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst-mac</td>
<td>If the dst-mac filter option is given, trace output is filtered on matching the given Destination MAC Address.</td>
</tr>
<tr>
<td>fip proto-code</td>
<td>If the fip proto-code filter option is given, trace output is filtered on matching the supported types.</td>
</tr>
<tr>
<td>src intf</td>
<td>If the src intf filter option is given, trace output is filtered on matching the incoming source interface.</td>
</tr>
<tr>
<td>src mac</td>
<td>If the src mac filter option is given, trace output is filtered on matching the given Source MAC Address.</td>
</tr>
<tr>
<td>vlan</td>
<td>If the vlan filter option is given, trace output is filtered on matching the given VLAN ID.</td>
</tr>
</tbody>
</table>

3.15.33.1 no debug fip-snooping packet

Use the `no debug fip-snooping packet` command in Privileged EXEC mode to disable FIP packet debug trace on transmit or receive path with different filter options configured.

**Format**
```
no debug fip-snooping packet [{transmit | receive | filter {dst-mac mac-addr | fip,proto-code 1-15 | src-intf slot/port | src-mac mac-addr | vlan 1-4093}]
```

**Mode**
- User EXEC
- Privileged EXEC

3.15.34 debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

**Default** disabled

**Format**
```
debug igmpsnooping packet
```

**Mode** Privileged EXEC

3.15.34.1 no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

**Format**
```
no debug igmpsnooping packet
```

**Mode** Privileged EXEC
3.15.35 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**
ddebug 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/SNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt TX
- Intf: 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX</td>
<td>A packet transmitted by the device.</td>
</tr>
<tr>
<td>Intf</td>
<td>The interface that the packet went out on. Format used is slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.</td>
</tr>
<tr>
<td>Src_Mac</td>
<td>Source MAC address of the packet.</td>
</tr>
<tr>
<td>Dest_Mac</td>
<td>Destination multicast MAC address of the packet.</td>
</tr>
<tr>
<td>Src_IP</td>
<td>The source IP address in the IP header in the packet.</td>
</tr>
<tr>
<td>Dest_IP</td>
<td>The destination multicast IP address in the packet.</td>
</tr>
</tbody>
</table>
| Type      | The type of IGMP packet. Type can be one of the following:
|           | - Membership Query – IGMP Membership Query
|           | - V1_Membership_Report – IGMP Version 1 Membership Report
|           | - V2_Leave_Group – IGMP Version 2 Leave Group
| Group     | Multicast group address in the IGMP header. |

3.15.35.1 no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

**Format**
n debug igmpsnooping transmit

**Mode**
Privileged EXEC

3.15.36 debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

**Default**

disabled

**Format**
d debug igmpsnooping packet receive

**Mode**
Privileged EXEC

A sample output of the trace message is shown below.

<15> JAN 01 02:45:06 192.168.17.29-1 IGMP/SNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt RX
- Intf: 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX</td>
<td>A packet received by the device.</td>
</tr>
<tr>
<td>Intf</td>
<td>The interface that the packet went out on. Format used is slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.</td>
</tr>
<tr>
<td>Src_Mac</td>
<td>Source MAC address of the packet.</td>
</tr>
<tr>
<td>Dest_Mac</td>
<td>Destination multicast MAC address of the packet.</td>
</tr>
<tr>
<td>Src_IP</td>
<td>The source IP address in the ip header in the packet.</td>
</tr>
<tr>
<td>Dest_IP</td>
<td>The destination multicast ip address in the packet.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of IGMP packet. Type can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Membership_Query – IGMP Membership Query</td>
</tr>
<tr>
<td></td>
<td>• V1_Membership_Report – IGMP Version 1 Membership Report</td>
</tr>
<tr>
<td></td>
<td>• V2_Membership_Report – IGMP Version 2 Membership Report</td>
</tr>
<tr>
<td></td>
<td>• V3_Membership_Report – IGMP Version 3 Membership Report</td>
</tr>
<tr>
<td></td>
<td>• V2_Leave_Group – IGMP Version 2 Leave Group</td>
</tr>
<tr>
<td>Group</td>
<td>Multicast group address in the IGMP header.</td>
</tr>
</tbody>
</table>

3.15.36.1 no debug igmpsnooping receive
This command disables tracing of received IGMP Snooping packets.

Format       no debug igmpsnooping receive
Mode         Privileged EXEC

3.15.37 debug ip acl
Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Default      disabled
Format        debug ip acl acl Number
Mode          Privileged EXEC

3.15.37.1 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

3.15.38 debug ip dvmrp packet
Use this command to trace DVMRP packet reception and transmission. receive traces only received DVMRP packets and transmit traces only transmitted DVMRP packets. When neither keyword is used in the command, then all DVMRP 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 dvmrp packet [receive | transmit]
Mode          Privileged EXEC
3.15.38.1  no debug ip dvmrp packet
Use this command to disable debug tracing of DVMRP packet reception and transmission.

Format  no debug ip dvmrp packet [receive | transmit]
Mode    Privileged EXEC

3.15.39  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

3.15.39.1  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

3.15.40  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

3.15.40.1  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

3.15.41  debug ip pimdm packet
Use this command to trace PIMDM packet reception and transmission. receive traces only received PIMDM packets and transmit traces only transmitted PIMDM packets. When neither keyword is used in the command, then all PIMDM 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 pimdm packet [receive | transmit]
Mode    Privileged EXEC
3.15.41.1 no debug ip pimdm packet
Use this command to disable debug tracing of PIMDM packet reception and transmission.

**Format**
no debug ip pimdm packet [receive | transmit]

**Mode**
Privileged EXEC

3.15.42 debug ip pimsm packet
Use this command to trace PIMSM packet reception and transmission. receive traces only received PIMSM packets and transmit traces only transmitted PIMSM packets. When neither keyword is used in the command, then all PIMSM 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 pimsm packet [receive | transmit]

**Mode**
Privileged EXEC

3.15.42.1 no debug ip pimsm packet
Use this command to disable debug tracing of PIMSM packet reception and transmission.

**Format**
no debug ip pimsm packet [receive | transmit]

**Mode**
Privileged EXEC

3.15.43 debug ip vrrp
Use this command to enable VRRP debug protocol messages.

**Default**
disabled

**Format**
debug ip vrrp

**Mode**
Privileged EXEC

3.15.43.1 no debug ip vrrp
Use this command to disable VRRP debug protocol messages.

**Format**
no debug ip vrrp

**Mode**
Privileged EXEC

3.15.44 debug ipv6 dhcp
This command displays “debug” information about DHCPv6 client activities and traces DHCPv6 packets to and from the local DHCPv6 client.

**Default**
disabled

**Format**
debug ipv6 dhcp

**Mode**
Privileged EXEC
3.15.44.1 no debug ipv6 dhcp
This command disables the display of “debug” trace output for DHCPv6 client activity.

**Format**  
no debug ipv6 dhcp

**Mode**  
Privileged EXEC

3.15.45 debug ipv6 mcache packet
Use this command for tracing MDATAv6 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 ipv6 mcache packet [receive | transmit]

**Mode**  
Privileged EXEC

3.15.45.1 no debug ipv6 mcache packet
Use this command to disable debug tracing of MDATAv6 packet reception and transmission.

**Format**  
no debug ipv6 mcache packet [receive | transmit]

**Mode**  
Privileged EXEC

3.15.46 debug ipv6 mld packet
Use this command to trace MLDv6 packet reception and transmission. receive traces only received MLDv6 packets and transmit traces only transmitted MLDv6 packets. When neither keyword is used in the command, then all MLDv6 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 ipv6 mld packet [receive | transmit]

**Mode**  
Privileged EXEC

3.15.46.1 no debug ipv6 mld packet
Use this command to disable debug tracing of MLDv6 packet reception and transmission.

**Format**  
no debug ipv6 mld packet [receive | transmit]

**Mode**  
Privileged EXEC

3.15.47 debug ipv6 ospfv3 packet
Use this command to enable IPv6 OSPFv3 packet debug trace.

**Default**  
disabled

**Format**  
debug ipv6 ospfv3 packet

**Mode**  
Privileged EXEC
3.15.47.1  no debug ipv6 ospfv3 packet

Use this command to disable tracing of IPv6 OSPFv3 packets.

**Format**  
no debug ipv6 ospfv3 packet

**Mode**  
Privileged EXEC

3.15.48  debug ipv6 pimdm packet

Use this command to trace PIMDMv6 packet reception and transmission. receive traces only received PIMDMv6 packets and transmit traces only transmitted PIMDMv6 packets. When neither keyword is used in the command, then all PIMDMv6 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 ipv6 pimdm packet [receive | transmit]

**Mode**  
Privileged EXEC

3.15.48.1  no debug ipv6 pimdm packet

Use this command to disable debug tracing of PIMDMv6 packet reception and transmission.

3.15.49  debug ipv6 pimsm packet

Use this command to trace PIMSMv6 packet reception and transmission. receive traces only received PIMSMv6 packets and transmit traces only transmitted PIMSMv6 packets. When neither keyword is used in the command, then all PIMSMv6 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 ipv6 pimsm packet [receive | transmit]

**Mode**  
Privileged EXEC

3.15.49.1  no debug ipv6 pimsm packet

Use this command to disable debug tracing of PIMSMv6 packet reception and transmission.

**Format**  
no debug ipv6 pimsm packet [receive | transmit]

**Mode**  
Privileged EXEC

3.15.50  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 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %
Pkt TX - Intf: 0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key: 0x36
3.15.50.1 no debug lacp packet
This command disables tracing of LACP packets.

<table>
<thead>
<tr>
<th>Format</th>
<th>no debug lacp packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.15.51 debug mldsnooping 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.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>debug mldsnooping packet [receive</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.15.51.1 no debug mldsnooping packet
Use this command to disable debug tracing of MLD snooping packet reception and transmission.

3.15.52 debug ospf packet
This command enables tracing of OSPF packets received and transmitted by the switch or, optionally, a virtual router can be specified.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>debug ospf packet</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

Sample outputs of the trace messages are shown below.

```<15> JAN 02 11:03:31 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25430 % Pkt RX - Intf:0/48 SrcIp:192.168.50.2 DestIp:224.0.0.5 AreaId:0.0.0.0 Type:HELLO NetMask:255.255.255.0 DesigRouter:0.0.0.0 Backup:0.0.0.0
```

```<15> JAN 02 11:03:35 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25431 % Pkt TX - Intf:0/48 SrcIp:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:DB_DSCR Mtu:1500 Options:E Flags: I/M/MS Seq:126166
```

```<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25434 % Pkt RX - Intf:0/48 SrcIp:192.168.50.2 DestIp:192.168.50.1 AreaId:0.0.0.0 Type:LS_REQ Length: 1500
```

```<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25435 % Pkt TX - Intf:0/48 SrcIp:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:LS_UPD Length: 1500
```

```<15> JAN 02 11:03:37 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25441 % Pkt TX - Intf:0/48 SrcIp:10.50.50.1 DestIp:224.0.0.6 AreaId:0.0.0.0 Type:LS_ACK Length: 1500
```

The following parameters are displayed in the trace message:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX/RX</td>
<td>TX refers to a packet transmitted by the device. RX refers to packets received by the device.</td>
</tr>
<tr>
<td>Intf</td>
<td>The interface that the packet came in or went out on. Format used is slot/port (internal interface number).</td>
</tr>
<tr>
<td>SrcIp</td>
<td>The source IP address in the IP header of the packet.</td>
</tr>
<tr>
<td>DestIp</td>
<td>The destination IP address in the IP header of the packet.</td>
</tr>
</tbody>
</table>
The remaining fields in the trace are specific to the type of OSPF Packet.

HELLO packet field definitions:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AreaId</td>
<td>The area ID in the OSPF header of the packet.</td>
</tr>
<tr>
<td>Type</td>
<td>Could be one of the following:</td>
</tr>
<tr>
<td></td>
<td>HELLO – Hello packet</td>
</tr>
<tr>
<td></td>
<td>DB_DSCR – Database descriptor</td>
</tr>
<tr>
<td></td>
<td>LS_REQ – LS Request</td>
</tr>
<tr>
<td></td>
<td>LS_UPD – LS Update</td>
</tr>
<tr>
<td></td>
<td>LS_ACK – LS Acknowledge</td>
</tr>
</tbody>
</table>

Netmask     | The netmask in the hello packet.                                           |
DesignRouter | Designated Router IP address.                                              |
Backup      | Backup router IP address.                                                  |

DB_DSCR packet field definitions:

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>MTU</td>
</tr>
<tr>
<td>Options</td>
<td>Options in the OSPF packet.</td>
</tr>
<tr>
<td>Flags</td>
<td>Could be one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>• I – Init</td>
</tr>
<tr>
<td></td>
<td>• M – More</td>
</tr>
<tr>
<td></td>
<td>• MS – Master/Slave</td>
</tr>
<tr>
<td>Seq</td>
<td>Sequence Number of the DD packet.</td>
</tr>
</tbody>
</table>

LS_REQ packet field definitions:

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>Length of packet</td>
</tr>
</tbody>
</table>

LS_UPD packet field definitions:

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>Length of packet</td>
</tr>
</tbody>
</table>

LS_ACK packet field definitions:

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>Length of packet</td>
</tr>
</tbody>
</table>
3.15.52.1  no debug ospf packet
This command disables tracing of OSPF packets.

<table>
<thead>
<tr>
<th>Format</th>
<th>no debug ospf packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.15.53  debug ospfv3 packet
Use this command to enable OSPFv3 packet debug trace.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>debug ospfv3 packet</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.15.53.1  no debug ospfv3 packet
Use this command to disable tracing of OSPFv3 packets.

<table>
<thead>
<tr>
<th>Format</th>
<th>no debug ospfv3 packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

3.15.54  debug ping packet
This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/service port for switching packages. For routing packages, pings are traced on the routing ports as well.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>debug ping packet</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

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: 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: 0/1(1), SRC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX/RX</td>
<td>TX refers to a packet transmitted by the device. RX refers to packets received by the device.</td>
</tr>
<tr>
<td>Intf</td>
<td>The interface that the packet came in or went out on. Format used is slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.</td>
</tr>
<tr>
<td>SRC_IP</td>
<td>The source IP address in the IP header in the packet.</td>
</tr>
<tr>
<td>DEST_IP</td>
<td>The destination IP address in the IP header in the packet.</td>
</tr>
<tr>
<td>Type</td>
<td>Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.</td>
</tr>
</tbody>
</table>
3.15.54.1 no debug ping packet
This command disables tracing of ICMP echo requests and responses.

Format no debug ping packet
Mode Privileged EXEC

3.15.55 debug rip packet
This command turns on tracing of RIP requests and responses. This command takes no options. The output is directed to the log file.

Default disabled
Format debug rip packet
Mode Privileged EXEC

A sample output of the trace message is shown below.

<15> JAN 01 00:35:15 192.168.17.29-1 RIP[181783160]: rip_map_debug.c(96) 775 %
Pkt RX on Intf: 0/1(1), Src_IP:43.1.1.1 Dest_IP:43.1.1.2
Rip_Version: RIPv2 Packet_Type: RIP_RESPONSE
ROUTE 1): Network: 10.1.1.0 Mask: 255.255.255.0 Metric: 1
ROUTE 2): Network: 40.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 3): Network: 10.50.50.0 Mask: 255.255.255.0 Metric: 1
ROUTE 4): Network: 41.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 5): Network: 42.0.0.0 Mask: 255.0.0.0 Metric: 1
Another 6 routes present in packet not displayed.

The following parameters are displayed in the trace message:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX/RX</td>
<td>TX refers to a packet transmitted by the device. RX refers to packets received by the device.</td>
</tr>
<tr>
<td>Intf</td>
<td>The interface that the packet came in or went out on. Format used is slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.</td>
</tr>
<tr>
<td>Src_IP</td>
<td>The source IP address in the IP header of the packet.</td>
</tr>
<tr>
<td>Dest_IP</td>
<td>The destination IP address in the IP header of the packet.</td>
</tr>
<tr>
<td>Rip_Version</td>
<td>RIP version used: RIPv1 or RIPv2.</td>
</tr>
<tr>
<td>Packet_Type</td>
<td>Type of RIP packet: RIP_REQUEST or RIP_RESPONSE.</td>
</tr>
<tr>
<td>Routes</td>
<td>Up to 5 routes in the packet are displayed in the following format:</td>
</tr>
<tr>
<td></td>
<td>Network: a.b.c.d Mask a.b.c.d Next_Hop a.b.c.d Metric a</td>
</tr>
<tr>
<td></td>
<td>The next hop is only displayed if it is different from 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td>For RIPv1 packets, Mask is always 0.0.0.0.</td>
</tr>
<tr>
<td>Number of routes not printed</td>
<td>Only the first five routes present in the packet are included in the trace. There is another notification of the number of additional routes present in the packet that were not included in the trace.</td>
</tr>
</tbody>
</table>
3.15.55.1 no debug rip packet
This command disables tracing of RIP requests and responses.

Format
no debug rip packet
Mode
Privileged EXEC

3.15.56 debug sflow packet
Use this command to enable sFlow debug packet trace.

Default
disabled
Format
debug sflow packet
Mode
Privileged EXEC

3.15.56.1 no debug sflow packet
Use this command to disable sFlow debug packet trace.

Format
no debug sflow packet
Mode
Privileged EXEC

3.15.57 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

3.15.57.1 no debug spanning-tree bpdu
This command disables tracing of spanning tree BPDUs.

Format
no debug spanning-tree bpdu
Mode
Privileged EXEC

3.15.58 debug spanning-tree bpdu receive
This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default
disabled
Format
debug spanning-tree bpdu receive
Mode
Privileged EXEC

A sample output of the trace message is shown below.

15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX - Intf: 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:
3.15.58.1  no debug spanning-tree bpdu receive
This command disables tracing of received spanning tree BPDUs.

Format  no debug spanning-tree bpdu receive
Mode    Privileged EXEC

3.15.59   debug spanning-tree bpdu transmit
This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default  disabled
Format   debug spanning-tree bpdu transmit
Mode     Privileged EXEC

A sample output of the trace message is shown below.

<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt TX - Intf: 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX</td>
<td>A packet received by the device.</td>
</tr>
<tr>
<td>Intf</td>
<td>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.</td>
</tr>
<tr>
<td>Source_Mac</td>
<td>Source MAC address of the packet.</td>
</tr>
<tr>
<td>Version</td>
<td>Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.</td>
</tr>
<tr>
<td>Root_Mac</td>
<td>MAC address of the CIST root bridge.</td>
</tr>
<tr>
<td>Root_Priority</td>
<td>Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.</td>
</tr>
<tr>
<td>Path_Cost</td>
<td>External root path cost component of the BPDU.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX</td>
<td>A packet transmitted by the device.</td>
</tr>
<tr>
<td>Intf</td>
<td>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.</td>
</tr>
<tr>
<td>Source_Mac</td>
<td>Source MAC address of the packet.</td>
</tr>
<tr>
<td>Version</td>
<td>Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.</td>
</tr>
<tr>
<td>Root_Mac</td>
<td>MAC address of the CIST root bridge.</td>
</tr>
<tr>
<td>Root_Priority</td>
<td>Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.</td>
</tr>
<tr>
<td>Path_Cost</td>
<td>External root path cost component of the BPDU.</td>
</tr>
</tbody>
</table>
3.15.59.1  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

3.15.60  debug tacacs
Use the debug tacacs packet command to turn on TACACS+ debugging.

    Format  debug tacacs {packet [receive | transmit] | accounting | authentication}
    Mode    Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet receive</td>
<td>Turn on TACACS+ receive packet debugs.</td>
</tr>
<tr>
<td>packet transmit</td>
<td>Turn on TACACS+ transmit packet debugs.</td>
</tr>
<tr>
<td>accounting</td>
<td>Turn on TACACS+ authentication debugging.</td>
</tr>
<tr>
<td>authentication</td>
<td>Turn on TACACS+ authorization debugging.</td>
</tr>
</tbody>
</table>

3.15.61  debug telnetd start
Use this command to start the debug telnet daemon. The debug telnet daemon gives access to a Linux shell prompt. The telnet user ID is "root". If the telnet daemon is already running when this command is issued, the command stops and restarts the telnet daemon.

    Format  debug telnetd start [password][port]
    Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>The optional telnet password. If no password is specified, the default password lvl7dbg is used.</td>
</tr>
<tr>
<td>port</td>
<td>The optional telnet port number. If no telnet port is specified, the default port 2323 is used.</td>
</tr>
</tbody>
</table>

3.15.62  debug telnetd stop
Use this command to stop the telnet daemon previously started by the debug telnetd start command. If the daemon is not running when this command is issued, the command has no effect.

    Format  debug telnetd stop
    Mode    Privileged EXEC

3.15.63  debug transfer
This command enables debugging for file transfers.

    Format  debug transfer
    Mode    Privileged EXEC
3.15.63.1  no debug transfer
This command disables debugging for file transfers.

Format  no debug transfer
Mode    Privileged EXEC

3.15.64  debug udld events
This command enables debugging for the UDLD events.

Default   Disabled
Format     debug udld events
Mode       Privileged EXEC

3.15.65  debug udld packet receive
This command enables debugging on the received UDLD PDU's.

Default   Disabled
Format     debug udld packet receive
Mode       Privileged EXEC

3.15.66  debug udld packet transmit
This command enables debugging on the transmitted UDLD PDU's.

Default   Disabled
Format     debug udld packet transmit
Mode       Privileged EXEC

3.15.67  show debugging
Use the show debugging command to display enabled packet tracing configurations.

Format     show debugging
Mode       Privileged EXEC

Example: The following shows example CLI display output for the command.
console# debug arp
Arp packet tracing enabled.

crsole# show debugging
Arp packet tracing enabled.
3.15.67.1  no show debugging
Use the no show debugging command to disable packet tracing configurations.

Format  no show debugging
Mode    Privileged EXEC

3.15.68  exception protocol
Use this command to specify the protocol used to store the core dump file.

This command is only available on selected Linux-based platforms.

Default  None
Format    exception protocol {nfs | tftp | ftp | local | usb | none}
Mode      Global Config

3.15.68.1  no exception protocol
Use this command to reset the exception protocol configuration to its factory default value.

This command is only available on Linux-based platforms.

Default  None
Format    no exception protocol
Mode      Global Config

3.15.69  exception dump tftp-server
Use this command to configure the IP address of a remote TFTP server in order to dump core files to an external server.

This command is only available on selected Linux-based platforms.

Default  None
Format    exception dump tftp-server {ip-address}
Mode      Global Config
3.15.69.1 no exception dump tftp-server
Use this command to reset the exception dump remote server configuration to its factory default value.

**NOTICE**
This command is only available on selected Linux-based platforms.

- **Default**: None
- **Format**: no exception dump tftp-server
- **Mode**: Global Config

3.15.70 exception dump nfs
Use this command to configure an NFS mount point in order to dump core file to the NFS file system.

**NOTICE**
This command is only available on selected Linux-based platforms.

- **Default**: None
- **Format**: exception dump nfs ip-address/dir
- **Mode**: Global Config

3.15.70.1 no exception dump nfs
Use this command to reset the exception dump NFS mount point configuration to its factory default value.

**NOTICE**
This command is only available on selected Linux-based platforms.

- **Default**: None
- **Format**: no exception dump nfs
- **Mode**: Global Config

3.15.71 exception dump filepath
Use this command to configure a file-path to dump core file to a TFTP server, NFS mount or USB device subdirectory.

**NOTICE**
This command is only available on selected Linux-based platforms.

- **Default**: None
- **Format**: exception dump filepath dir
- **Mode**: Global Config
3.15.71.1 no exception dump filepath

Use this command to reset the exception dump filepath configuration to its factory default value.

**NOTICE** This command is only available on selected Linux-based platforms.

Default: None

Format: exception dump filepath

Mode: Global Config

3.15.72 exception core-file

Use this command to configure a prefix for a core-file name. The core file name is generated with the prefix as follows:

If hostname is selected:

file-name-prefix_hostname_Time_Stamp.bin

If hostname is not selected:

file-name-prefix_MAC_Address_Time_Stamp.bin

If hostname is configured the core file name takes the hostname, otherwise the core-file names uses the MAC address when generating a core dump file. The prefix length is 15 characters.

**NOTICE** This command is only available on selected Linux-based platforms.

Default: Core

Format: exception core-file {file-name-prefix | hostname | time-stamp}  

Mode: Global Config

3.15.72.1 no exception core-file

Use this command to reset the exception core file prefix configuration to its factory default value. The hostname and time-stamp are disabled.

**NOTICE** This command is only available on selected Linux-based platforms.

Default: Core

Format: no exception core-file

Mode: Global Config

3.15.73 exception switch-chip-register

This command enables or disables the switch-chip-register dump in case of an exception. The switch-chip-register dump is taken only for a master unit and not for member units.

**NOTICE** This command is only available on selected Linux-based platforms.
3.15.74 exception dump ftp-server
This command configures the IP address of remote FTP server to dump core files to an external server. If the username and password are not configured, the switch uses anonymous FTP. (The FTP server should be configured to accept anonymous FTP.)

Default None
Format exception dump ftp-server ip-address [{username user-name password password}]
Mode Global Config

3.15.74.1 no exception dump ftp-server
This command resets exception dump remote FTP server configuration to its factory default value. This command also resets the FTP username and password to empty string.

Default None
Format no exception dump ftp-server
Mode Global Config

3.15.75 exception dump compression
This command enables compression mode.

Default Enabled
Format exception dump compression
Mode Global Config

3.15.75.1 no exception dump compression
This command disables compression mode.

Default None
Format no exception compression
Mode Global Config

3.15.76 exception dump stack-ip-address protocol
This command configures protocol (dhcp or static) to be used to configure service port when a unit has crashed. If configured as dhcp then the unit gets the IP address from dhcp server available in the network.

Default dhcp
Format exception dump stack-ip-address protocol {dhcp | static}
Mode Global Config
3.15.76.1 no exception dump stack-ip-address protocol
This command resets stack IP protocol configuration (dhcp or static) to its default value.

Default: None
Format: no exception dump stack-ip-address protocol
Mode: Global Config

3.15.77 exception dump stack-ip-address add
This command adds static IP address to be assigned to individual unit’s service port in the stack when the switch has crashed. This IP address is used to perform the core dump.

Default: None
Format: exception dump stack-ip-address add ip-address netmask [gateway]
Mode: Global Config

3.15.78 exception dump stack-ip-address remove
This command removes stack IP address configuration. If this IP address is assigned to any unit in the stack then this IP is removed from the unit.

Default: None
Format: exception dump stack-ip-address remove ip-address netmask
Mode: Global Config

3.15.79 exception nmi
This command enables or disables taking core dump in case of NMI occurs.

Default: Disable
Format: exception nmi {enable | disable}
Mode: Global Config

3.15.80 write core
Use the write core command to generate a core dump file on demand. The write core test command is helpful when testing the core dump setup. For example, if the TFTP protocol is configured, write core test communicates with the TFTP server and informs the user if the TFTP server can be contacted. Similarly, if protocol is configured as nfs, this command mounts and unmounts the file system and informs the user of the status.

write core reloads the switch which is useful when the device malfunctions, but has not crashed.

For write core test, the destination file name is used for the TFTP test. Optionally, you can specify the destination file name when the protocol is configured as TFTP.

This command is only available on selected Linux-based platforms.
3.15.81 debug exception

The command displays core dump features support.

Default: None
Format: debug exception
Mode: Privileged EXEC

3.15.82 show exception

Use this command to display the configuration parameters for generating a core dump file.

Example: The following shows an example of this command.

```
show exception
```

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coredump file name</td>
<td>core</td>
</tr>
<tr>
<td>Coredump filename uses hostname</td>
<td>False</td>
</tr>
<tr>
<td>Coredump filename uses time-stamp</td>
<td>TRUE</td>
</tr>
<tr>
<td>TFTP Server Address</td>
<td>TFTP server configuration</td>
</tr>
<tr>
<td>FTP Server IP</td>
<td>FTP server configuration</td>
</tr>
<tr>
<td>FTP user name</td>
<td>FTP user name</td>
</tr>
<tr>
<td>FTP password</td>
<td>FTP password</td>
</tr>
<tr>
<td>NFS Mount point</td>
<td>NFS mount point config.</td>
</tr>
<tr>
<td>File path</td>
<td>Remote file path</td>
</tr>
<tr>
<td>Core File name prefix</td>
<td>Core file name config.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Core file name contains hostname if enabled.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Core file name contains timestamp if enabled.</td>
</tr>
<tr>
<td>Switch Chip Register Dump</td>
<td>Switch chip register dump config.</td>
</tr>
<tr>
<td>Compression mode</td>
<td>TRUE/ FALSE</td>
</tr>
<tr>
<td>Stack IP Address Protocol</td>
<td>DHCP/ Static</td>
</tr>
<tr>
<td>Stack IP Address</td>
<td>List of IP addresses configured</td>
</tr>
</tbody>
</table>

3.15.83 show exception core-dump-file

This command displays core dump files existing on the local file system.

Default: None
Format: show exception core-dump-file
Mode: Privileged EXEC, Config Mode
3.15.84  show exception log
This command displays core dump traces on the local file system.

Default          None
Format            show exception log [previous]
Mode              Privileged EXEC, Config Mode

3.15.85  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

3.15.85.1  no logging persistent
Use this command to disable the persistent logging in the switch.

Format            no logging persistent
Mode              Global Config

3.15.86  mbuf
Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format            mbuf (falling-threshold | rising threshold | severity)
Mode              Global Config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rising Threshold</td>
<td>The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).</td>
</tr>
<tr>
<td>Falling Threshold</td>
<td>The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity level at which Mbuf logs messages. The range is 1 to 7. The default is 5 (L7_LOG_SEVERITY_NOTICE).</td>
</tr>
</tbody>
</table>

3.15.87  show mbuf
Use this command to display the memory buffer (MBUF) Utilization Monitoring parameters.

Format            show mbuf
Mode              Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rising Threshold</td>
<td>The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).</td>
</tr>
</tbody>
</table>
3.15.88  show mbuf total

Use this command to display memory buffer (MBUF) information.

**Format**  
show mbuf total

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mbufs Total</td>
<td>Total number of message buffers in the system.</td>
</tr>
<tr>
<td>Mbufs Free</td>
<td>Number of message buffers currently available.</td>
</tr>
<tr>
<td>Mbufs Rx Used</td>
<td>Number of message buffers currently in use.</td>
</tr>
<tr>
<td>Total Rx Norm Alloc Attempts</td>
<td>Number of times the system tried to allocate a message buffer allocation of class RX Norm.</td>
</tr>
<tr>
<td>Total Rx Mid2 Alloc Attempts</td>
<td>Number of times the system tried to allocate a message buffer allocation of class RX Mid2.</td>
</tr>
<tr>
<td>Total Rx Mid1 Alloc Attempts</td>
<td>Number of times the system tried to allocate a message buffer allocation of class RX Mid1.</td>
</tr>
<tr>
<td>Total Rx Mid0 Alloc Attempts</td>
<td>Number of times the system tried to allocate a message buffer allocation of class RX Mid0.</td>
</tr>
<tr>
<td>Total Rx High Alloc Attempts</td>
<td>Number of times the system tried to allocate a message buffer allocation of class RX High.</td>
</tr>
<tr>
<td>Total Tx Alloc Attempts</td>
<td>Number of times the system tried to allocate a message buffer allocation of class TX.</td>
</tr>
<tr>
<td>Total Rx Norm Alloc Failures</td>
<td>Number of message buffer allocation failures for RX Norm class of message buffer.</td>
</tr>
<tr>
<td>Total Rx Mid2 Alloc Failures</td>
<td>Number of message buffer allocation failures for RX Mid2 class of message buffer.</td>
</tr>
<tr>
<td>Total Rx Mid1 Alloc Failures</td>
<td>Number of message buffer allocation failures for RX Mid1 class of message buffer.</td>
</tr>
<tr>
<td>Total Rx Mid0 Alloc Failures</td>
<td>Number of message buffer allocation failures for RX Mid0 class of message buffer.</td>
</tr>
<tr>
<td>Total Rx High Alloc Failures</td>
<td>Number of message buffer allocation failures for RX High class of message buffer.</td>
</tr>
<tr>
<td>Total Tx Alloc Failures</td>
<td>Number of message buffer allocation failures for TX class of message buffer.</td>
</tr>
</tbody>
</table>

3.15.89  show msg-queue

Use this command to display the message queues.

**Default**  
None

**Format**  
show msg-queue

**Mode**  
Privileged EXEC mode
3.15.90  debug packet-trace
Use this command to enable traces for the packet trace feature.

Default: None
Format: debug packet-trace
Mode: Privileged Exec

3.15.91  packet-trace eth
Use this command to specify the ethernet packet fields for a packets for which a trace profile is required. If the optional vlan parameter is not specified, the PVID/internal VLAN associated with the ingress port (specified in the show packet-trace command) is used in the VLAN tag.

Default: None
Format: packet-trace eth src-mac src-mac dst-mac dst-mac vlan vlan
Mode: Privileged Exec

3.15.92  packet-trace ipv4
Use this command to specify the IPv4 packet header fields.

Default: None
Format: packet-trace ipv4 src-ip src-ip dst-ip dst-ip tos tos
Mode: Privileged Exec

3.15.93  packet-trace ipv6
Use this command to specify the IPv6 packet header fields.

Default: None
Format: packet-trace ipv6 src-ip src-ip dst-ip dst-ip tos tos
Mode: Privileged Exec

3.15.94  packet-trace l4
Use this command to specify TCP packet fields.

Default: None
Format: packet-trace l4 src-port src-port dst-port dst-port
Mode: Privileged Exec

3.15.95  show packet-trace ecmp
Use this command for getting a summary (link utilization percentage) for all complete packets present in the PCAP file (uploaded onto the system using the copy command).

Default: None
Format: show packet-trace ecmp prefix/prefix-length port unit/slot/port pcap summary
Mode: Privileged Exec
3.15.96  show packet-trace lag

Use this command for getting a summary (link utilization percentage) for all complete packets present in the PCAP file (uploaded onto the system using the copy command).

Default None
Format show packet-trace lag lag-id port unit/slot/port pcap summary
Mode Privileged Exec

Example:
(Routing)#show packet-trace lag 1 port 0/1 pcap summary

LAG ................................. 3/1
Link State............................... Up
Admin Mode............................ Enabled
Type..................................... Static
Port-channel Min-links.................. 1
Load Balance Option.................... 3
(Src/Dest MAC, VLAN, EType, incoming port)

<table>
<thead>
<tr>
<th>Mbr</th>
<th>Device/Port</th>
<th>Speed</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/3</td>
<td>actor/long</td>
<td>10G Full</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>partner/long</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/2</td>
<td>actor/long</td>
<td>10G Full</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>partner/long</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

LAG 1 member port link utilization %:
암호화된 정보
Total number of valid packets in pcap file: 20
Member port 0/3 utilization: 20%
Member port 0/4 utilization: 80%

3.15.97  show packet-trace packet-data

Use this command to dump all the configured packet header fields.

Default By default, all packet fields are set to 0.
Format show packet-trace packet-data
Mode Privileged Exec

Example:
DUT#show packet-trace packet-data

L2 Header fields:
-------------------
Src MAC: 00 00 00 0a 0b 0c
Dst MAC: 00 00 00 0d 0e 0f
VLAN: 10

L3 Header fields:
-------------------
IPv4:
Src IP: 10.0.10.1
Dst IP: 10.0.10.10
TOS: 0

IPv6:
Src IP: 4001::1/8
Dst IP: 5001::1/8
Traffic Class: 0

L4 header fields:
-------------------------------
Src Port: 80
Dst Port: 80

3.15.98 show packet-trace port

Use this command for getting detailed information for the maximum packets in the PCAP file.

Default: None
Format: show packet-trace port unit/slot/port pcap detailed maxpkts
Mode: Privileged Exec

Example:
DUT#show packet-trace port 0/1 pcap detailed 5

Packet fields:
src-Mac ------------------ 00:00:00:00:00:0a
dst-mac ------------------ 00:00:00:00:00:0b
vlan ------------------ 10
src-ip ------------------ 10.0.1.10
dst-ip ------------------ 10.0.1.20

LAG Destination member port
-------------------------------
Lag 1 0/4

Packet fields:
src-Mac ------------------ 00:00:00:00:00:0c
dst-mac ------------------ 00:00:00:00:00:0d
vlan ------------------ 10
src-ip ------------------ 10.0.1.10
dst-ip ------------------ 10.0.1.20

LAG Destination member port
-------------------------------
Lag 1 0/3

Packet fields:
src-Mac ------------------ 00:00:00:00:00:0e
dst-mac ------------------ 00:00:00:00:00:0f
vlan ------------------ 10
src-ip ------------------ 10.0.1.10
dst-ip ------------------ 10.0.1.20

LAG Destination member port
-------------------------------
Lag 1 0/2

Packet fields:
src-Mac ------------------ 00:00:00:00:00:1a
dst-mac ------------------ 00:00:00:00:00:1b
vlan ------------------ 10
src-ip ------------------ 10.0.1.10
dst-ip ------------------ 10.0.1.20

LAG Destination member port
---                       ------------------
Lag 1                        0/4

Packet fields:
src-Mac  -----------------  00:00:00:00:00:1c
dst-mac  -----------------  00:00:00:00:00:1d
vlan     -----------------  10
src-ip   -----------------  10.0.1.10
dst-ip   -----------------  10.0.1.20

LAG Destination member port
---                       ------------------
Lag 1                        0/3

3.15.99  show packet-trace port eth

Use this command to retrieve the trace profile for an ethernet packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information.

Default                  None
Format                   show packet-trace port unit/slot/port eth
Mode                     Privileged Exec

Example:
(Routing)# show packet-trace port 0/1 eth

LAG Destination member port
---                       ------------------
Lag 1                        0/3

LAG ............................ 3/1
Link State........................ Up
Admin Mode......................... Enabled
Type............................... Static
Port-channel Min-links........... 1
Load Balance Option............... 3
(Src/Dest MAC, VLAN, EType, incoming port)

Mbr Device/ Port Port
Ports Timeout Speed Active
---                      --- --- ---
0/3 actor/long 10G Full True
                 partner/long
0/2 actor/long 10G Full True
                 partner/long

3.15.100  show packet-trace port ipv4

Use this command to retrieve the trace profile for an IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for an IP packet, both the Ethernet and IP packet fields need to be configured.

Default                  None
Format                   show packet-trace port unit/slot/port ipv4
Mode                     Privileged Exec
**Example:**

(Routing)# show packet-trace port 0/1 ipv4

<table>
<thead>
<tr>
<th>ECMP</th>
<th>Egress port</th>
<th>Next Hop IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.2/16</td>
<td>0/4</td>
<td>3.3.3.3</td>
</tr>
</tbody>
</table>

ECMP routes to 10.0.0.2/16:

- via 3.3.3.3 on interface 0/4
- via 2.2.2.2 on interface 0/5

### 3.15.101 show packet-trace port ipv6

Use this command to retrieve the trace profile for an IPv6 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for an IP packet, both the ethernet and IP packet fields need to be configured.

**Default** None

**Format**

```
show packet-trace port unit/slot/port ipv6
```

**Mode** Privileged Exec

**Example:**

(Routing)# show packet-trace port 0/1 uipv6

<table>
<thead>
<tr>
<th>ECMP</th>
<th>Egress port</th>
<th>Next Hop IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>6001::200/64</td>
<td>0/4</td>
<td>8001::200</td>
</tr>
</tbody>
</table>

ECMP routes to 6001::200/64:

- via 8001::200 on interface 0/32
- via 7001::200 on interface 0/5

### 3.15.102 show packet-trace port tcpv4

Use this command to get the egress LAG member port for a L3 IPv4 packet specified by the configured packet fields and to get the egressing ECMP route link information (physical port) for a TCP-IPv4 packet specified by the configured packet fields. Note that, in order to get the trace profile for a TCP packet, the L2, L3, and L4 packet fields need to be configured.

**Default** None

**Format**

```
show packet-trace port unit/slot/port tcpv4
```

**Mode** Privileged Exec

### 3.15.103 show packet-trace port tcpv6

Use this command to retrieve the trace profile for a TCP-IPv6 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for a TCP packet, the ethernet, IP and L4 packet fields need to be configured.

**Default** None

**Format**

```
show packet-trace port unit/slot/port tcpv6
```

**Mode** Privileged Exec
3.15.104  show packet-trace port udpv4
Use this command to retrieve the trace profile for a UDP-IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for a UDP packet, the ethernet, IP and L4 packet fields need to be configured.

Default None
Format show packet-trace port unit/slot/port udpv4
Mode Privileged Exec

3.15.105  show packet-trace port udpv6
Use this command to retrieve the trace profile for a UDP-IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for a UDP packet, the ethernet, IP and L4 packet fields need to be configured.

Default None
Format show packet-trace port unit/slot/port udpv6
Mode Privileged Exec

3.15.106  clear packet-trace packet-data
Use this command to clear the configured packet header fields.

Format clear packet-trace packet-data
Mode Privileged Exec

3.15.107  session start
Use this command to initiate a console session from the stack master to another unit in the stack, or from a member unit to a manager or another member unit. During the session, troubleshooting and debugging commands can be issued on the member unit, and the output displays the relevant information from the member unit specified in the session. Commands are displayed on the member unit using the user help option ?.

Default Disable
Format session start {unit unit-number | manager}
Mode Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit</td>
<td>Use to connect to the specified unit from the stack master.</td>
</tr>
<tr>
<td>manager</td>
<td>Use to connect directly to the manager unit from any member unit without entering the manager’s unit number.</td>
</tr>
</tbody>
</table>

3.15.108  session stop
Use this command to terminate a session started from a manager to a member, a member to a member, or a member to manager that was started with the session start command.

Default Disable
Format session stop {unit unit-number | manager}
Mode Global Config
### 3.15.109 watchdog clear

This command clears the watchdog settings and history and resets the timeout interval to the default value.

**Format**

```
watchdog clear
```  

**Mode**

Privileged EXEC

### 3.15.110 watchdog disable

This command disables watchdog services. Watchdog is automatically changed (that is, no reboot is required).

**Default**

Disabled

**Format**

```
watchdog disable
```  

**Mode**

Privileged EXEC

### 3.15.111 watchdog enable

This command enables watchdog services. Watchdog services give FASTPATH the ability to recover when it is no longer executing properly. When a recovery is attempted, debug information is saved and the switch is reset.

**Default**

Disabled

**Format**

```
watchdog enable
```  

**Mode**

Privileged EXEC

### 3.16 BCM Shell Command

The BCM (SDK) shell is mainly used for debugging the Broadcom SDK. BCM shell commands can be executed directly from the CLI without entering the BCM shell itself by using the keyword `drivshell` before the BCM command. However, you can also enter the BCM shell to directly execute any of the BCM commands on the shell using the `bcmsh` command.

#### 3.16.1 bcmsh

The `bcmsh` command is used to enter into the BCM shells from Privileged EXEC mode. Only users with Level 15 permissions can execute this command. Management is blocked during this mode; the user is notified and asked whether to continue. This command is only supported on the serial console and not via telnet/ssh.

**Format**

```
bcmsh
```  

**Mode**

Privileged EXEC

---

**NOTICE**

To exit the shell and return to the CLI, enter `exit`.
3.17 Cable Test Command
The cable test feature enables you to determine the cable connection status on a selected port.

3.17.1 cablestatus
This command returns the status of the specified port.

Format: cablestatus slot/port
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Status</td>
<td>One of the following statuses is returned:</td>
</tr>
<tr>
<td></td>
<td>• Normal: The cable is working correctly.</td>
</tr>
<tr>
<td></td>
<td>• Open: The cable is disconnected or there is a faulty connector.</td>
</tr>
<tr>
<td></td>
<td>• Short: There is an electrical short in the cable.</td>
</tr>
<tr>
<td></td>
<td>• Cable Test Failed: The cable status could not be determined. The cable may in fact be working.</td>
</tr>
<tr>
<td></td>
<td>• Crosstalk: There is crosstalk present on the cable.</td>
</tr>
<tr>
<td></td>
<td>• No Cable: There is no cable present.</td>
</tr>
<tr>
<td>Cable Length</td>
<td>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.</td>
</tr>
</tbody>
</table>

3.18 sFlow Commands
sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

3.18.1 sflow poller
A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance on an interface or range of interfaces for this data source if rcvr_idx is valid.

Format: sflow poller {rcvr-index | interval poll-interval}
Mode: Interface Config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver Index</td>
<td>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.</td>
</tr>
<tr>
<td>Poll Interval</td>
<td>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.</td>
</tr>
</tbody>
</table>
The sFlow task is heavily loaded when the sFlow polling interval is configured at the minimum value (i.e., one second for all the sFlow supported interfaces). In this case, the sFlow task is always busy collecting the counters on all the configured interfaces. This can cause the device to hang for some time when the user tries to configure or issue show sFlow commands. To overcome this situation, sFlow polling interval configuration on an interface or range of interfaces is controlled as mentioned below:

- The maximum number of allowed interfaces for the polling intervals max (1, (interval – 10)) to min ((interval + 10), 86400) is:
  \[ \text{interval} \times 5 \]
- For every one second increment in the polling interval that is configured, the number of allowed interfaces that can be configured increases by 5.

### 3.18.1.1 no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

**Format**

```
no sflow poller [interval]
```

**Mode**

Interface Config

### 3.18.2 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 ip | port port}
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Receiver Owner</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Receiver Timeout</strong></td>
<td>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 0-2147483647 seconds. The default is zero (0).</td>
</tr>
<tr>
<td><strong>No Timeout</strong></td>
<td>The configured entry will be in the config until you explicitly removes the entry.</td>
</tr>
<tr>
<td><strong>Receiver Max Datagram Size</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Receiver IP</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Receiver Port</strong></td>
<td>The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.</td>
</tr>
</tbody>
</table>
3.18.2.1 no sflow receiver
Use this command to set the sFlow collector parameters back to the defaults.

**Format**
```
no sflow receiver index (ip ip-address | maxdatagram size | owner string timeout interval | port 14-port)
```

**Mode**
Global Config

3.18.3 sflow receiver owner timeout
Use this command to configure a receiver as a timeout entry. As the sFlow receiver is configured as a timeout entry, information related to sampler and pollers are also shown in the running-config and are retained after reboot.

If a receiver is configured with a specific value, these configurations will not be shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

**Format**
```
sflow receiver index owner owner-string timeout
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>Receiver index identifier. The range is 1 to 8.</td>
</tr>
<tr>
<td>Receiver Owner</td>
<td>The owner name corresponds to the receiver name. 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.</td>
</tr>
</tbody>
</table>

3.18.4 sflow receiver owner notimeout
Use this command to configure a receiver as a non-timeout entry. Unlike entries configured with a specific timeout value, this command will be shown in show running-config and retained after reboot. As the sFlow receiver is configured as a non-timeout entry, information related to sampler and pollers will also be shown in the running-config and will be retained after reboot.

If a receiver is configured with a specific value, these configurations will not be shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

**Format**
```
sflow receiver index owner owner-string notimeout
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>Receiver index identifier. The range is 1 to 8.</td>
</tr>
<tr>
<td>Receiver Owner</td>
<td>The owner name corresponds to the receiver name. 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.</td>
</tr>
</tbody>
</table>
3.18.5  **sflow remote-agent ip**
Use this command to assign an IPv4 address to a remote agent. When sFlow hardware sampling is enabled, the switch/hardware sends sampled packets encapsulated in sFlow custom packet to this IP address.

**Default**
0.0.0.0

**Format**
sflow remote-agent index ip  ipv4-address

**Mode**
Global Config

3.18.5.1  **no sflow remote-agent ip**
Use this command to remove the remote agent IPv4 address.

**Format**
no sflow remote-agent index ip

**Mode**
Global Config

3.18.6  **sflow remote-agent monitor-session**
Use this command to assign the monitor ID (MTP) for the remote agent session. The destination port is an outgoing interface for sFlow sampled packets. The sflow sampled packets are sent to all the configured destination ports, irrespective of monitor session index.

**Default**
0 for both monitor session and destination port

**Format**
sflow remote-agent index monitor-session session id range 1-4  destination interface unit/slot/port

**Mode**
Global Config

3.18.6.1  **no sflow remote-agent monitor-session**
This command removes the remote-agent configuration.

**Format**
no sflow remote-agent index monitor-session

**Mode**
Global Config

3.18.7  **sflow remote-agent port**
This command configures the destination UDP port for the remote-agent.

**Default**
16343

**Format**
sflow remote-agent index port value

**Mode**
Global Config
3.18.7.1 no sflow remote-agent port
This command removes remote agent port configuration.

**Format**
no sflow remote-agent port

**Mode**
Global Config

3.18.8 sflow sampler
A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance on an interface or range of interfaces for this data source if `rcvr_idx` is valid.

**Format**
sflow sampler `{rcvr-index | rate sampling-rate | maxheadersize size}`

**Mode**
Interface Config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver Index</td>
<td>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.</td>
</tr>
<tr>
<td>Maxheadersize</td>
<td>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.</td>
</tr>
<tr>
<td>Sampling Rate</td>
<td>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.</td>
</tr>
</tbody>
</table>

3.18.8.1 no sflow sampler
Use this command to reset the sFlow sampler instance to the default settings.

**Format**
no sflow sampler `{rcvr-index | rate sampling-rate | maxheadersize size}`

**Mode**
Interface Config

3.18.9 sflow sampler rate
Use this command to set the sampling rate for ingress/egress/flow-based sampling on this interface.

**Default**
0 for the ingress sampling rate.

**Format**
sflow sampler rate `value` {ingress | egress | flow-based}

**Mode**
Interface Config
3.18.9.1 no sflow sample rate
Use this command to remove the sampling rate for ingress/egress/flow-based sampling on this interface.

**Format**
```
no sflow sampler rate value {ingress | egress | flow-based}
```

**Mode**
Interface Config

3.18.10 sflow sampler remote-agent
Use this command to enable a new sFlow sampler remote agent instance for this data source.

**Default**
None

**Format**
```
sflow sampler remote-agent index
```

**Mode**
Interface Config

3.18.10.1 no sflow sampler remote-agent
Use this command to disable an sFlow sampler remote agent instance for this data source.

**Format**
```
no sflow sampler remote-agent
```

**Mode**
Interface Config

3.18.11 sflow sampler filter ip access-group
Use this command to enable flow-based ingress packet sampling on an interface for an IP ACL identified by ACL name or ACL ID. The packet matching the defined flow/ACL may get sampled by this configuration.

**Default**
None

**Format**
```
sflow sampler filter ip access-group {aclid | aclName}
```

**Mode**
Interface Config

3.18.11.1 no sflow sampler filter ip access-group
Use this command to disable the sFlow for an IP ACL identified by name or ID on the interface.

**Format**
```
no sflow sampler filter ip access-group {aclid | aclName}
```

**Mode**
Interface Config

3.18.12 sflow sampler filter mac access-group
Use this command to enable flow-based ingress packet sampling on an interface for MAC ACL identified by ACL name. The packet matching the defined flow/ACL may get sampled by this configuration.

**Default**
None

**Format**
```
sflow sampler filter mac access-group aclName
```

**Mode**
Interface Config
3.18.12.1 no sflow sampler filter mac access-group
Use this command to disable the sFlow for MAC ACL identified by name on the interface.

Format no sflow sampler filter mac access-group
Mode Interface Config

3.18.13 sflow source-interface
Use this command to specify the physical or logical interface to use as the sFlow client source interface. If configured, the address of source Interface is used for all sFlow communications between the sFlow receiver and the sFlow client. Otherwise there is no change in behavior. If the configured interface is down, the sFlow client falls back to normal behavior.

Format sflow source-interface {slot/port | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}
Mode Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>VLAN or port-based routing interface.</td>
</tr>
<tr>
<td>loopback-id</td>
<td>Configures the loopback interface to use as the source IP address. The range of the loopback ID is 0 to 7.</td>
</tr>
<tr>
<td>tunnel-id</td>
<td>Configures the tunnel interface to use as the source IP address. The range of the tunnel ID is 0 to 7.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Configures the VLAN interface to use as the source IP address. The range of the VLAN ID is 1 to 4093.</td>
</tr>
</tbody>
</table>

3.18.13.1 no sflow source-interface
Use this command to reset the sFlow source interface to the default settings.

Format no sflow source-interface
Mode Global Config

3.18.14 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sFlow Version</td>
<td>Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where:</td>
</tr>
<tr>
<td></td>
<td>• MIB Version: 1.3, the version of this MIB.</td>
</tr>
<tr>
<td></td>
<td>• Organization: Broadcom Corp.</td>
</tr>
<tr>
<td></td>
<td>• Revision: 1.0</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address associated with this agent.</td>
</tr>
</tbody>
</table>
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
```

### 3.18.15 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
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poller Data Source</td>
<td>The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.</td>
</tr>
<tr>
<td>Receiver Index</td>
<td>The sFlowReceiver associated with this sFlow counter poller.</td>
</tr>
<tr>
<td>Poller Interval</td>
<td>The number of seconds between successive samples of the counters associated with this data source.</td>
</tr>
</tbody>
</table>

### 3.18.16 show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

**Format**

```
show sflow receivers [index]
```

**Mode**

```
Privileged EXEC
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver Index</td>
<td>The sFlow Receiver associated with the sampler/poller.</td>
</tr>
<tr>
<td>Owner String</td>
<td>The identity string for receiver, the entity making use of this sFlowRcvrTable entry.</td>
</tr>
<tr>
<td>Time Out</td>
<td>The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver. The no timeout value of this parameter means that the sFlow receiver is configured as a non-timeout entry.</td>
</tr>
<tr>
<td>Max Datagram Size</td>
<td>The maximum number of bytes that can be sent in a single sFlow datagram.</td>
</tr>
<tr>
<td>Port</td>
<td>The destination Layer4 UDP port for sFlow datagrams.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The sFlow receiver IP address.</td>
</tr>
<tr>
<td>Address Type</td>
<td>The sFlow receiver IP address type. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.</td>
</tr>
<tr>
<td>Datagram Version</td>
<td>The sFlow protocol version to be used while sending samples to sFlow receiver.</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the `show sflow receivers` command.

```
(switch) #show sflow receivers 1
Receiver Index......................... 1
Owner String............................ tulasi
Time out................................. 0
IP Address................................ 0.0.0.0
Address Type............................ 1
Port.................................. 6343
Datagram Version....................... 5
Maximum Datagram Size............... 1400
```
**Example:** The following examples show CLI display output for the command when a receiver is configured as a non-timeout entry.

(FASTPATH Routing) #show sflow receivers

<table>
<thead>
<tr>
<th>Rcvr Index</th>
<th>Owner String</th>
<th>Timeout</th>
<th>Max Dgram Size</th>
<th>Port</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>tulasi</td>
<td>No Timeout</td>
<td>1400</td>
<td>6343</td>
<td>0.0.0.0 &lt;= No Timeout string</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>0</td>
<td>1400</td>
<td>6343</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>0</td>
<td>1400</td>
<td>6343</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>0</td>
<td>1400</td>
<td>6343</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>0</td>
<td>1400</td>
<td>6343</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>0</td>
<td>1400</td>
<td>6343</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>0</td>
<td>1400</td>
<td>6343</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>0</td>
<td>1400</td>
<td>6343</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

(FASTPATH Routing) #show sflow receivers 1

Receiver Index.................................. 1
Owner String................................... tulasi
Timeout........................................ No Timeout <= No Timeout string is added
IP Address...................................... 0.0.0.0
Address Type.................................. 1
Port............................................. 6343
Datagram Version.............................. 5
Maximum Datagram Size......................... 1400

3.18.17 show sflow remote-agents

Use this command to display the details for configured sFlow remote agents.

**Format**

show sflow remote-agents

**Mode**

Privileged EXEC

**Example:**

(Routing) (Config)#show sflow remote-agents

<table>
<thead>
<tr>
<th>Rem Agent Index</th>
<th>Port</th>
<th>IP Address</th>
<th>Monitor Session</th>
<th>Dest. Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>16343</td>
<td>1.1.1.1</td>
<td>1</td>
<td>0/4</td>
</tr>
<tr>
<td>2</td>
<td>26343</td>
<td>2.2.1.1</td>
<td>2</td>
<td>0/8</td>
</tr>
<tr>
<td>3</td>
<td>16343</td>
<td>0.0.0.0</td>
<td>2</td>
<td>0/8</td>
</tr>
<tr>
<td>4</td>
<td>16343</td>
<td>0.0.0.0</td>
<td>2</td>
<td>0/8</td>
</tr>
</tbody>
</table>

3.18.18 show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

**Format**

show sflow samplers

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampler Data Source</td>
<td>The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.</td>
</tr>
<tr>
<td>Receiver Index</td>
<td>The sFlowReceiver configured for this sFlow sampler.</td>
</tr>
<tr>
<td>Remote Agent</td>
<td>The remote agent instance index number.</td>
</tr>
<tr>
<td>Ingress Sampling Rate</td>
<td>The sampling rate for the ingress.</td>
</tr>
</tbody>
</table>
### Example:

```
(Routing) (Config)# show sflow samplers
```

<table>
<thead>
<tr>
<th>Sampler</th>
<th>Receiver</th>
<th>Remote</th>
<th>Ingress Sampling Rate</th>
<th>Egress Sampling Rate</th>
<th>Max Header Size</th>
<th>IP ACL</th>
<th>MAC ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source</td>
<td>Agent</td>
<td>Ingress</td>
<td>Flow Rate</td>
<td>Egress Rate</td>
<td>Max Size</td>
<td>IP</td>
<td>MAC</td>
</tr>
<tr>
<td>0/1</td>
<td>1</td>
<td>2</td>
<td>1024</td>
<td>2048</td>
<td>4096</td>
<td>128</td>
<td>1001</td>
</tr>
</tbody>
</table>

#### 3.18.19 show sflow source-interface

Use this command to display the sFlow source interface configured on the switch.

**Format**

```
show sflow source-interface
```

**Mode**

Privileged EXEC

### Field Description

- **sFlow Client Source Interface**: The interface ID of the physical or logical interface configured as the sFlow client source interface.
- **sFlow Client Source IPv4 Address**: The IP address of the interface configured as the sFlow client source interface.

#### Example:

```
(Routing) # show sflow source-interface
sFlow Client Source Interface................. (not configured)
```

### 3.19 Switch Database Management Template Commands

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

---

**NOTICE**

If you attach a unit to a stack and its template does not match the stack’s template, then the new unit will automatically reboot using the template used by other stack members. To avoid the automatic reboot, you may first set the template to the template used by existing members of the stack. Then power off the new unit, attach it to the stack, and power it on.
3.19.1  sd़m prefer

Use this command to change the template that will be active after the next reboot. The keywords are as follows:

• **dual-ipv4-and-ipv6**—Filters subsequent template choices to those that support both IPv4 and IPv6. The default template maximizes the number of IPv4 and IPv6 unicast routes, while limiting the number of ECMP next hops in each route to 4. The data-center template supports increases the number of ECMP next hops to 32. The alpm and alpm-mls-data-center templates accommodate larger routes. The values for the alpm and alpm-mls-data-center templates are shown below:

  dual-ipv4-and-ipv6 alpm:

  - ARP Entries: 2560
  - IPv4 Unicast Routes: 32768
  - IPv6 NDP Entries: 2560
  - IPv6 Unicast Routes: 24576
  - ECMP Next Hops: 48
  - IPv4 Multicast Routes: 0
  - IPv6 Multicast Routes: 0

  dual-ipv4-and-ipv6 alpm-mls-data-center:

  - ARP Entries: 2560
  - IPv4 Unicast Routes: 32768
  - IPv6 NDP Entries: 2560
  - IPv6 Unicast Routes: 24576
  - ECMP Next Hops: 16
  - IPv4 Multicast Routes: 0
  - IPv6 Multicast Routes: 0

• **ipv4-routing**—Filters subsequent template choices to those that support IPv4, and not IPv6. The IPv4-routing default template maximizes the number of IPv4 unicast routes, while limiting the number of ECMP next hops in each route to 4. The data-center default template supports increases the number of ECMP next hops to 32 and reduces the number of routes. The data-center plus template increases the number of ECMP next hops to 32 while keeping the maximum IPv4 routes.

---

**NOTICE**

After setting the template, you must reboot in order for the configuration change to take effect.

---

**Default**

dual IPv4 and IPv6 template

**Format**

```
  sdm prefer {dual-ipv4-and-ipv6 {default|data-center} | ipv4-routing {default|data-center {default|plus}}}
```

**Mode**

Global Config
3.19.1.1 no sdm prefer

Use this command to revert to the default template after the next reboot.

**Format**

no sdm prefer

**Mode**

Global Config

3.19.2 show sdm prefer

Use this command to view the currently active SDM template and its scaling parameters, or to view the scaling parameters for an inactive template. When invoked with no optional keywords, this command lists the currently active template and the template that will become active on the next reboot, if it is different from the currently active template. If the system boots with a non-default template, and you clear the template configuration, either using `no sdm prefer` or by deleting the startup configuration, `show sdm prefer` lists the default template as the next active template. To list the scaling parameters of a specific template, use that template's keyword as an argument to the command.

Use the optional keywords to list the scaling parameters of a specific template.

**Format**

show sdm prefer [dual-ipv4-and-ipv6 {default|data-center}] | ipv4-routing {default | data-center {default|plus}}]

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dual-ipv4-and-ipv6 default</td>
<td>(Optional) List the scaling parameters for the template supporting IPv4 and IPv6.</td>
</tr>
<tr>
<td>dual-ipv4-and-ipv6 data-center</td>
<td>(Optional) List the scaling parameters for the Dual IPv4 and IPv6 template supporting more ECMP next hops.</td>
</tr>
<tr>
<td>ipv4-routing default</td>
<td>(Optional) List the scaling parameters for the IPv4-only template maximizing the number of unicast routes.</td>
</tr>
<tr>
<td>ipv4-routing data-center default</td>
<td>(Optional) List the scaling parameters for the IPv4-only template supporting more ECMP next hops.</td>
</tr>
<tr>
<td>ipv4-routing data-center plus</td>
<td>(Optional) List the scaling parameters for the IPv4-only template maximizing the number of unicast routes and also supporting more ECMP next hops.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Entries</td>
<td>The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.</td>
</tr>
<tr>
<td>IPv4 Unicast Routes</td>
<td>The maximum number of IPv4 unicast forwarding table entries.</td>
</tr>
<tr>
<td>IPv6 NDP Entries</td>
<td>The maximum number of IPv6 Neighbor Discovery Protocol (NDP) cache entries.</td>
</tr>
<tr>
<td>IPv6 Unicast Routes</td>
<td>The maximum number of IPv6 unicast forwarding table entries.</td>
</tr>
<tr>
<td>ECMP Next Hops</td>
<td>The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.</td>
</tr>
</tbody>
</table>

**Example:** This example shows the current SDM template. The user has not changed the next active SDM template.

(router)# show sdm prefer

The current template is the Dual IPv4 and IPv6 template.

ARP Entries................................. 6144
IPv4 Unicast Routes....................... 8160
IPv6 NDP Entries........................... 2560
IPv6 Unicast Routes....................... 4096
Now the user sets the next active SDM template.

```
(router) # configure
(router) (Config)#sdm prefer ipv4-routing data-center default
```

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload. Use `show sdm prefer` to see what SDM preference is currently active.

```
(router) (Config)#ex
```

```
(router) #show sdm prefer
```

The current template is the Dual IPv4 and IPv6 template.

```
ARP Entries................................. 6144
IPv4 Unicast Routes........................ 8160
IPv6 NDP Entries............................ 2560
IPv6 Unicast Routes........................ 4096
ECMP Next Hops.............................. 4
IPv4 Multicast Routes....................... 1536
IPv6 Multicast Routes....................... 512
```

On the next reload, the template will be the IPv4 Data Center template.

```
(router) #
```

To list the scaling parameters for the data center template, invoke the command with the ipv4-routing data-center default keywords.

```
(router) #show sdm prefer ipv4-routing data-center default
```

```
ARP Entries................................. 6144
IPv4 Unicast Routes........................ 8160
IPv6 NDP Entries............................ 0
IPv6 Unicast Routes........................ 0
ECMP Next Hops.............................. 16
IPv4 Multicast Routes....................... 2048
IPv6 Multicast Routes....................... 0
```

### 3.20 Remote Monitoring Commands
Remote Monitoring (RMON) is a method of collecting a variety of data about network traffic. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).

---

**NOTICE**
There is no configuration command for ether stats and high capacity ether stats. The data source for ether stats and high capacity ether stats are configured during initialization.
3.20.1  rmon alarm

This command sets the RMON alarm entry in the RMON alarm MIB group.

Format  
```
   rmon alarm alarm number variable sample interval {absolute|delta} rising-threshold
   value [rising-event-index] falling-threshold value [falling-event-index] [startup
   {rising|falling|rising-falling}] [owner string]
```

Mode  
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Index</td>
<td>An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.</td>
</tr>
<tr>
<td>Alarm Variable</td>
<td>The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.</td>
</tr>
<tr>
<td>Alarm Interval</td>
<td>The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.</td>
</tr>
<tr>
<td>Alarm Absolute Value</td>
<td>The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.</td>
</tr>
<tr>
<td>Alarm Rising Threshold</td>
<td>The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.</td>
</tr>
<tr>
<td>Alarm Rising Event Index</td>
<td>The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.</td>
</tr>
<tr>
<td>Alarm Falling Threshold</td>
<td>The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.</td>
</tr>
<tr>
<td>Alarm Falling Event Index</td>
<td>The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.</td>
</tr>
<tr>
<td>Alarm Startup Alarm</td>
<td>The alarm that may be sent. Possible values are rising, falling or both rising-falling. The default is rising-falling.</td>
</tr>
<tr>
<td>Alarm Owner</td>
<td>The owner string associated with the alarm entry. The default is monitorAlarm.</td>
</tr>
</tbody>
</table>

Example: The following shows an example of the command.

```
(FASTPATH Routing) (Config)# rmon alarm 1 ifInErrors.2 30 absolute rising-threshold 100 1 falling-threshold 10 2 startup rising owner myOwner
```
### 3.20.1.1 no rmon alarm

This command deletes the RMON alarm entry.

**Format**

```
no rmon alarm alarm number
```

**Mode**

Global Config

**Example:** The following shows an example of the command.

```
(FASTPATH Routing) (Config)# no rmon alarm 1
```

### 3.20.2 rmon hcalarm

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

**Format**

```
rmon hcalarm alarm number variable sample interval {absolute|delta} rising-threshold high value low value status {positive|negative} [rising-event-index] falling-threshold high value low value status {positive|negative} [falling-event-index] [startup {rising|falling|rising-falling}] [owner string]
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Capacity Alarm Index</td>
<td>An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.</td>
</tr>
<tr>
<td>High Capacity Alarm Variable</td>
<td>The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.</td>
</tr>
<tr>
<td>High Capacity Alarm Interval</td>
<td>The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.</td>
</tr>
<tr>
<td>High Capacity Alarm Sample Type</td>
<td>The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are Absolute Value or Delta Value. The default is Absolute Value.</td>
</tr>
<tr>
<td>High Capacity Alarm Absolute Value</td>
<td>The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.</td>
</tr>
<tr>
<td>High Capacity Alarm Absolute Status</td>
<td>This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are valueNotAvailable, valuePositive, or valueNegative. The default is valueNotAvailable.</td>
</tr>
<tr>
<td>High Capacity Alarm Startup Alarm</td>
<td>High capacity alarm startup alarm that may be sent. Possible values are rising, falling, or rising-falling. The default is rising-falling.</td>
</tr>
<tr>
<td>High Capacity Alarm Rising-Threshold Absolute Value Low</td>
<td>The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.</td>
</tr>
<tr>
<td>High Capacity Alarm Rising-Threshold Absolute Value High</td>
<td>The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.</td>
</tr>
<tr>
<td>High Capacity Alarm Rising-Threshold Value Status</td>
<td>This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.</td>
</tr>
</tbody>
</table>
**Example:** The following shows an example of the command.

```
(FASTPATH Routing) (Config)# rmon hcalarm 1 ifInOctets.1 30 absolute rising-threshold high 1 low 100 status positive 1 falling-threshold high 1 low 10 status positive startup rising owner myOwner
```

3.20.2.1 no rmon hcalarm

This command deletes the rmon hcalarm entry.

**Format**  
no rmon hcalarm *alarm* *number*

**Mode**  
Global Config

**Example:** The following shows an example of the command.

```
(FASTPATH Routing) (Config)# no rmon hcalarm 1
```

3.20.3 rmon event

This command sets the RMON event entry in the RMON event MIB group.

**Format**  
rmon event *event* *number* [description *string*|log|owner *string*|trap *community*]

**Mode**  
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Index</td>
<td>An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.</td>
</tr>
<tr>
<td>Event Description</td>
<td>A comment describing the event entry. The default is alarmEvent.</td>
</tr>
</tbody>
</table>
### Event Type
The type of notification that the probe makes about the event. Possible values are None, Log, SNMP Trap, Log and SNMP Trap. The default is None.

### Event Owner
Owner string associated with the entry. The default is monitorEvent.

### Event Community
The SNMP community specific by this octet string which is used to send an SNMP trap. The default is public.

**Example:** The following shows an example of the command.

```
(FASTPATH Routing) (Config)# rmon event 1 log description test
```

3.20.3.1 no rmon event

This command deletes the rmon event entry.

**Format**
no rmon event event number

**Mode**
Global Config

**Example:** The following shows an example of the command.

```
(FASTPATH Routing) (Config)# no rmon event 1
```

3.20.4 rmon collection history

This command sets the history control parameters of the RMON historyControl MiB group.

---

**NOTICE** This command is not supported on interface range. Each RMON history control collection entry can be configured on only one interface. If you try to configure on multiple interfaces, DUT displays an error.

**Format**
rmon collection history index number [buckets number|interval interval in sec|owner string]

**Mode**
Interface Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History Control Index</td>
<td>An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.</td>
</tr>
<tr>
<td>History Control Data Source</td>
<td>The source interface for which historical data is collected.</td>
</tr>
<tr>
<td>History Control Buckets Requested</td>
<td>The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.</td>
</tr>
<tr>
<td>History Control Buckets Granted</td>
<td>The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.</td>
</tr>
<tr>
<td>History Control Interval</td>
<td>The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.</td>
</tr>
<tr>
<td>History Control Owner</td>
<td>The owner string associated with the history control entry. The default is monitorHistory-Control.</td>
</tr>
</tbody>
</table>
**Example:** The following shows an example of the command.

```plaintext
(FASTPATH Routing) (Interface 0/1)# rmon collection history 1 buckets 10 interval 30 owner myOwner
```

**Error:** 'rmon collection history' is not supported on range of interfaces.

### 3.20.4.1 no rmon collection history

This command will delete the history control group entry with the specified index number.

**Format**

```
no rmon collection history index number
```

**Mode**

```
Interface Config
```

**Example:** The following shows an example of the command.

```plaintext
(FASTPATH Routing) (Interface 0/1-0/10)# no rmon collection history 1
```

### 3.20.5 show rmon

This command displays the entries in the RMON alarm table.

**Format**

```
show rmon {alarms | alarm alarm-index}
```

**Mode**

```
Privileged EXEC
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Index</td>
<td>An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.</td>
</tr>
<tr>
<td>Alarm Variable</td>
<td>The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.</td>
</tr>
<tr>
<td>Alarm Interval</td>
<td>The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.</td>
</tr>
<tr>
<td>Alarm Absolute Value</td>
<td>The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.</td>
</tr>
<tr>
<td>Alarm Rising Threshold</td>
<td>The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.</td>
</tr>
<tr>
<td>Alarm Rising Event Index</td>
<td>The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.</td>
</tr>
<tr>
<td>Alarm Falling Threshold</td>
<td>The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.</td>
</tr>
<tr>
<td>Alarm Falling Event Index</td>
<td>The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.</td>
</tr>
<tr>
<td>Alarm Startup Alarm</td>
<td>The alarm that may be sent. Possible values are rising, falling or both rising-falling. The default is rising-falling.</td>
</tr>
<tr>
<td>Alarm Owner</td>
<td>The owner string associated with the alarm entry. The default is monitorAlarm.</td>
</tr>
</tbody>
</table>

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

```plaintext
(FASTPATH Routing) #show rmon alarms
```

<table>
<thead>
<tr>
<th>Index</th>
<th>OID</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>alarmInterval.1</td>
<td>MibBrowser</td>
</tr>
<tr>
<td>2</td>
<td>alarmInterval.1</td>
<td>MibBrowser</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(FASTPATH Routing) #show rmon alarm 1

Alarm 1

------------------
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold: 1
Falling Threshold: 1
Rising Event: 1
Falling Event: 2
Owner: MibBrowser

3.20.6  show rmon collection history
This command displays the entries in the RMON history control table.

Format  show rmon collection history [interfaces slot/port]
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History Control Index</td>
<td>An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.</td>
</tr>
<tr>
<td>History Control Data Source</td>
<td>The source interface for which historical data is collected.</td>
</tr>
<tr>
<td>History Control Buckets Requested</td>
<td>The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.</td>
</tr>
<tr>
<td>History Control Buckets Granted</td>
<td>The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.</td>
</tr>
<tr>
<td>History Control Interval</td>
<td>The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.</td>
</tr>
<tr>
<td>History Control Owner</td>
<td>The owner string associated with the history control entry. The default is monitorHistoryControl.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show rmon collection history

<table>
<thead>
<tr>
<th>Index</th>
<th>Interface</th>
<th>Interval</th>
<th>Requested Samples</th>
<th>Granted Samples</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0/1</td>
<td>30</td>
<td>10</td>
<td>10</td>
<td>myowner</td>
</tr>
<tr>
<td>2</td>
<td>0/1</td>
<td>1800</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>3</td>
<td>0/2</td>
<td>30</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>4</td>
<td>0/2</td>
<td>1800</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>5</td>
<td>0/3</td>
<td>30</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>6</td>
<td>0/3</td>
<td>1800</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>7</td>
<td>0/4</td>
<td>30</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>8</td>
<td>0/4</td>
<td>1800</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>9</td>
<td>0/5</td>
<td>30</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>10</td>
<td>0/5</td>
<td>1800</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
<tr>
<td>11</td>
<td>0/6</td>
<td>30</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(FASTPATH Routing) #show rmon collection history interfaces 0/1

<table>
<thead>
<tr>
<th>Index</th>
<th>Interface</th>
<th>Interval</th>
<th>Requested Samples</th>
<th>Granted Samples</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0/1</td>
<td>30</td>
<td>10</td>
<td>10</td>
<td>myowner</td>
</tr>
<tr>
<td>2</td>
<td>0/1</td>
<td>1800</td>
<td>50</td>
<td>10</td>
<td>monitorHistoryControl</td>
</tr>
</tbody>
</table>

3.20.7 show rmon events

This command displays the entries in the RMON event table.

Format: `show rmon events`

Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Index</td>
<td>An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.</td>
</tr>
<tr>
<td>Event Description</td>
<td>A comment describing the event entry. The default is alarmEvent.</td>
</tr>
<tr>
<td>Event Type</td>
<td>The type of notification that the probe makes about the event. Possible values are None, Log, SNMP Trap, Log and SNMP Trap. The default is None.</td>
</tr>
<tr>
<td>Event Owner</td>
<td>Owner string associated with the entry. The default is monitorEvent.</td>
</tr>
<tr>
<td>Event Community</td>
<td>The SNMP community specific by this octet string which is used to send an SNMP trap. The default is public.</td>
</tr>
<tr>
<td>Owner</td>
<td>Event owner. The owner string associated with the entry.</td>
</tr>
<tr>
<td>Last time sent</td>
<td>The last time over which a log or a SNMP trap message is generated.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) # show rmon events

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Type</th>
<th>Community</th>
<th>Owner</th>
<th>Last time sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>test</td>
<td>log</td>
<td>public</td>
<td>MIB</td>
<td>0 days 0 h:0 m:0 s</td>
</tr>
</tbody>
</table>

3.20.8 show rmon history

This command displays the specified entry in the RMON history table.

Format: `show rmon history index {errors | other | throughput | high-capacity}[period seconds]`

Mode: Privileged EXEC
### Example: The following shows example CLI display output for the command.

(Routing) #show rmon history 1 errors

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sample set</strong></td>
<td>The index (identifier) for the RMON history entry within the RMON history group. Each such entry defines a set of samples at a particular interval for an interface on the device.</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>The owner string associated with the history control entry. The default is monitorHistoryControl.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>The interface that was sampled.</td>
</tr>
<tr>
<td><strong>Interval</strong></td>
<td>The time between samples, in seconds.</td>
</tr>
<tr>
<td><strong>Requested Samples</strong></td>
<td>The number of samples (intervals) requested for the RMON history entry.</td>
</tr>
<tr>
<td><strong>Granted Samples</strong></td>
<td>The number of samples granted for the RMON history entry.</td>
</tr>
<tr>
<td><strong>Maximum Table Size</strong></td>
<td>Maximum number of entries that the history table can hold.</td>
</tr>
</tbody>
</table>

**Common Fields**

**Sample set**
The index (identifier) for the RMON history entry within the RMON history group. Each such entry defines a set of samples at a particular interval for an interface on the device.

**Owner**
The owner string associated with the history control entry. The default is monitorHistoryControl.

**Interface**
The interface that was sampled.

**Interval**
The time between samples, in seconds.

**Requested Samples**
The number of samples (intervals) requested for the RMON history entry.

**Granted Samples**
The number of samples granted for the RMON history entry.

**Maximum Table Size**
Maximum number of entries that the history table can hold.

**Output for Errors Parameter**

**Time**
Time at which the sample is collected, displayed as period seconds.

**CRC Align**
Number of CRC align errors.

**Undersize Packets**
Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).

**Oversize Packets**
Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).

**Fragments**
Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).

**Jabbers**
Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).

**Output for Others Parameter**

**Time**
Time at which the sample is collected, displayed as period seconds.

**Dropped Collisions**
Total number of dropped collisions.

**Output for Throughput Parameter**

**Time**
Time at which the sample is collected, displayed as period seconds.

**Octets**
Total number of octets received on the interface.

**Packets**
Total number of packets received (including error packets) on the interface.

**Broadcast**
Total number of good broadcast packets received on the interface.

**Multicast**
Total number of good multicast packets received on the interface.

**Util**
Port utilization of the interface associated with the history index specified.

**Output for High-Capacity Parameter**

**Time**
Time at which the sample is collected, displayed as period seconds.

**Overflow Pkts**
The number of times the associated packet counter has overflowed.

**Pkts**
The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

**Overflow Octets**
The number of times the associated octet counter has overflowed.

**Octets**
The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Requested Samples: 10  Granted Samples: 10
Maximum table size: 1758

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

(Routing) #show rmon history 1 throughput

Sample set: 1  Owner: myowner
Interface: 1/0/1  Interval: 30
Requested Samples: 10  Granted Samples: 10
Maximum table size: 1758

<table>
<thead>
<tr>
<th>Time</th>
<th>Octets</th>
<th>Packets</th>
<th>Broadcast</th>
<th>Multicast</th>
<th>Util</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 01 1970 21:41:43</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:42:14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:42:44</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:43:14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:43:44</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:44:14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:44:45</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:45:15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:45:45</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Jan 01 1970 21:46:15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

(Routing) #show rmon history 1 other

Sample set: 1  Owner: myowner
Interface: 1/0/1  Interval: 30
Requested Samples: 10  Granted Samples: 10
Maximum table size: 1758

<table>
<thead>
<tr>
<th>Time</th>
<th>Dropped</th>
<th>Collisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 01 1970 21:41:43</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:42:14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:42:44</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:43:14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:43:44</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:44:14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:44:45</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:45:15</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:45:45</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 01 1970 21:46:15</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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

(Routing) #show rmon history 1 high-capacity

Sample set: 1  Owner: monitorHistoryControl
Interface: 0/1  Interval: 30
Requested Samples: 50  Granted Samples: 10
Maximum table size: 414

3.20.9  show rmon log

This command displays the entries in the RMON log table.

Format  show rmon log [event-index]
Mode Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum table size</td>
<td>Maximum number of entries that the log table can hold.</td>
</tr>
<tr>
<td>Event</td>
<td>Event index for which the log is generated.</td>
</tr>
<tr>
<td>Description</td>
<td>A comment describing the event entry for which the log is generated.</td>
</tr>
<tr>
<td>Time</td>
<td>Time at which the event is generated.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show rmon log

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
</table>

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

(FASTPATH Routing) #show rmon log 1

Maximum table size: 10

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
</table>

3.20.10  show rmon statistics interfaces

This command displays the RMON statistics for the given interfaces.

Format  show rmon statistics interfaces unit/slot/port
Mode  Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>unit/slot/port</td>
</tr>
<tr>
<td>Dropped</td>
<td>Total number of dropped events on the interface.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(Routing) # show rmon statistics interfaces 1/0/1
Port: 1/0/1
Dropped: 0
Packets: 0
Broadcast: 0 Multicast: 0
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 0 65 - 127 Octets: 0
128 - 255 Octets: 0 256 - 511 Octets: 0

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octets</td>
<td>Total number of octets received on the interface.</td>
</tr>
<tr>
<td>Packets</td>
<td>Total number of packets received (including error packets) on the interface.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Total number of good broadcast packets received on the interface.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Total number of good multicast packets received on the interface.</td>
</tr>
<tr>
<td>CRC Align Errors</td>
<td>Total number of packets received have a length (excluding framing bits, including FCS octets) of between 64 and 1518 octets inclusive.</td>
</tr>
<tr>
<td>Collisions</td>
<td>Total number of collisions on the interface.</td>
</tr>
<tr>
<td>Undersize Pkts</td>
<td>Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>Oversize Pkts</td>
<td>Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>Fragments</td>
<td>Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>Jabbers</td>
<td>Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).</td>
</tr>
<tr>
<td>64 Octets</td>
<td>Total number of packets which are 64 octets in length (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>65-127 Octets</td>
<td>Total number of packets which are between 65 and 127 octets in length (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>128-255 Octets</td>
<td>Total number of packets which are between 128 and 255 octets in length (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>256-511 Octets</td>
<td>Total number of packets which are between 256 and 511 octets in length (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>512-1023 Octets</td>
<td>Total number of packets which are between 512 and 1023 octets in length (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>1024-1518 Octets</td>
<td>Total number of packets which are between 1024 and 1518 octets in length (excluding framing bits, including FCS octets).</td>
</tr>
<tr>
<td>HC Overflow Pkts</td>
<td>Total number of times the packet counter has overflowed.</td>
</tr>
<tr>
<td>HC Overflow Octets</td>
<td>Total number of times the octet counter has overflowed.</td>
</tr>
<tr>
<td>HC Overflow Pkts 64 Octets</td>
<td>The number of times the associated 64-octet counter has overflowed.</td>
</tr>
<tr>
<td>HC Overflow Pkts 65 - 127 Octets</td>
<td>The number of times the associated 65–127 octet counter has overflowed.</td>
</tr>
<tr>
<td>HC Overflow Pkts 128 - 255 Octets</td>
<td>The number of times the associated 128–255 octet counter has overflowed.</td>
</tr>
<tr>
<td>HC Overflow Pkts 256 - 511 Octets</td>
<td>The number of times the associated 256–511 octet counter has overflowed.</td>
</tr>
<tr>
<td>HC Overflow Pkts 512 - 1023 Octets</td>
<td>The number of times the associated 512–1023 octet counter has overflowed.</td>
</tr>
<tr>
<td>HC Overflow Pkts 1024 - 1518 Octets</td>
<td>The number of times the associated 1024–1518 octet counter has overflowed.</td>
</tr>
</tbody>
</table>
3.20.11  show rmon hcalarms

This command displays the entries in the RMON high-capacity alarm table.

Format:  
show rmon {hcalarms|hcalarm [alarm index]}

Mode:  
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Capacity Alarm Index</td>
<td>An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.</td>
</tr>
<tr>
<td>High Capacity Alarm Variable</td>
<td>The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.</td>
</tr>
<tr>
<td>High Capacity Alarm Interval</td>
<td>The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.</td>
</tr>
<tr>
<td>High Capacity Alarm Sample Type</td>
<td>The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are Absolute Value or Delta Value. The default is Absolute Value.</td>
</tr>
<tr>
<td>High Capacity Alarm Absolute Value</td>
<td>The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.</td>
</tr>
<tr>
<td>High Capacity Alarm Absolute Status</td>
<td>This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueObject). Possible status types are valueNotAvailable, valuePositive, or valueNegative. The default is valueNotAvailable.</td>
</tr>
<tr>
<td>High Capacity Alarm Startup Alarm</td>
<td>High capacity alarm startup alarm that may be sent. Possible values are rising, falling, or rising-falling. The default is rising-falling.</td>
</tr>
<tr>
<td>High Capacity Alarm Rising-Threshold Absolute Value Low</td>
<td>The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.</td>
</tr>
<tr>
<td>High Capacity Alarm Rising-Threshold Absolute Value High</td>
<td>The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.</td>
</tr>
<tr>
<td>High Capacity Alarm Rising-Threshold Value Status</td>
<td>This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are valueNotAvailable, valuePositive, or valueNegative. The default is valuePositive.</td>
</tr>
<tr>
<td>High Capacity Alarm Falling-Threshold Absolute Value Low</td>
<td>The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

```
(FASTPATH Routing) #show rmon hcalarms

<table>
<thead>
<tr>
<th>Index</th>
<th>OID</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>alarmInterval.1</td>
<td>MibBrowser</td>
</tr>
<tr>
<td>2</td>
<td>alarmInterval.1</td>
<td>MibBrowser</td>
</tr>
</tbody>
</table>
```

```
(FASTPATH Routing) #show rmon hcalarm 1

Alarm  1
--------
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold High: 0
Rising Threshold Low: 1
Rising Threshold Status: Positive
Falling Threshold High: 0
Falling Threshold Low: 1
Falling Threshold Status: Positive
Rising Event: 1
Falling Event: 2
Startup Alarm: Rising-Falling
Owner: MibBrowser
```
3.21 Statistics Application Commands

The statistics application gives you the ability to query for statistics on port utilization, flow-based and packet reception on programmable time slots. The statistics application collects the statistics at a configurable time range. You can specify the port number(s) or a range of ports for statistics to be displayed. The configured time range applies to all ports. Detailed statistics are collected between a specified time range in date and time format. You can define the time range as having an absolute time entry and/or a periodic time. For example, you can specify the statistics to be collected and displayed between 9:00 12 NOV 2011 (START) and 21:00 12 NOV 2012 (END) or schedule it on every Mon, Wed, and Fri 9:00 (START) to 21:00 (END).

You can receive the statistics in the following ways:
- User requests through the CLI for a set of counters.
- Configuring the device to display statistics using syslog or email alert. The syslog or email alert messages are sent by the statistics application at END time.

You can configure the device to display statistics on the console. The collected statistics are presented on the console at END time.

3.21.1 stats group

This command creates a new group with the specified id or name and configures the time range and the reporting mechanism for that group.

**Format**

```plaintext
stats group group id|name timerange time range name name reporting list of reporting methods
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group ID, name</td>
<td>Name of the group of statistics or its identifier to apply on the interface. The range is:</td>
</tr>
<tr>
<td></td>
<td>1 received</td>
</tr>
<tr>
<td></td>
<td>2 received-errors</td>
</tr>
<tr>
<td></td>
<td>3 transmitted</td>
</tr>
<tr>
<td></td>
<td>4 transmitted-errors</td>
</tr>
<tr>
<td></td>
<td>5 received-transmitted</td>
</tr>
<tr>
<td></td>
<td>6 port-utilization</td>
</tr>
<tr>
<td></td>
<td>7 congestion</td>
</tr>
<tr>
<td></td>
<td>The default is None.</td>
</tr>
<tr>
<td>time range name</td>
<td>Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.</td>
</tr>
<tr>
<td>list of reporting methods</td>
<td>Report the statistics to the configured method. The range is:</td>
</tr>
<tr>
<td></td>
<td>0. none</td>
</tr>
<tr>
<td></td>
<td>1 console</td>
</tr>
<tr>
<td></td>
<td>2 syslog</td>
</tr>
<tr>
<td></td>
<td>3 e-mail</td>
</tr>
<tr>
<td></td>
<td>The default is None.</td>
</tr>
</tbody>
</table>

**Example:** The following shows examples of the command.

(FASTPATH Routing) (Config)# stats group received timerange test reporting console email syslog

(FASTPATH Routing) (Config)# stats group received-errors timerange test reporting email syslog

(FASTPATH Routing) (Config)# stats group received-transmitted timerange test reporting none
3.21.1.1 **no stats group**
This command deletes the configured group.

**Format**
no stats group *group id|name*

**Mode**
Global Config

**Example:** The following shows examples of the command.

```
(FASTPATH Routing) (Config)# no stats group received
(FASTPATH Routing) (Config)# no stats group received-errors
(FASTPATH Routing) (Config)# no stats group received-transmitted
```

3.21.2 **stats flow-based**
This command configures flow based statistics rules for the given parameters over the specified time range. Only an IPv4 address is allowed as source and destination IP address.

**Format**
```
stats flow-based rule-id timerange time range name [{srcip ip-address} {dstip ip-address} {srctcpport portid} {dsttcpport portid} {srcudpport portid} {dstudpport portid}]
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule ID</td>
<td>The flow-based rule ID. The range is 1 to 16. The default is None.</td>
</tr>
<tr>
<td>time range name</td>
<td>Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.</td>
</tr>
<tr>
<td>srcip ip-address</td>
<td>The source IP address.</td>
</tr>
<tr>
<td>dstip ip-address</td>
<td>The destination IP address.</td>
</tr>
<tr>
<td>srctcpport portid</td>
<td>The source TCP port number.</td>
</tr>
<tr>
<td>dsttcpport portid</td>
<td>The destination TCP port number.</td>
</tr>
<tr>
<td>srcudpport portid</td>
<td>The source UDP port number.</td>
</tr>
<tr>
<td>dstudpport portid</td>
<td>The destination UDP port number.</td>
</tr>
</tbody>
</table>

**Example:** The following shows examples of the command.

```
(FASTPATH Routing) (Config)#stats flow-based 1 timerange test srcip 1.1.1.1 dstip 2.2.2.2 srctcpport 1234 dsttcpport 123 srcudpport 123 dstudpport 123

(FASTPATH Routing) (Config)#stats flow-based 2 timerange test srcip 1.1.1.1 dstip 2.2.2.2 srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport 123
```
3.21.2.1 no stats flow-based
This command deletes flow-based statistics.

Format stats flow-based rule-id
Mode Global Config

Example: The following shows examples of the command.
(FASTPATH Routing) (Config)# no stats flow-based 1
(FASTPATH Routing) (Config)# no stats flow-based 2

3.21.3 stats flow-based reporting
This command configures the reporting mechanism for all the flow-based rules configured on the system. There is no per flow-based rule reporting mechanism. Setting the reporting method as none resets all the reporting methods.

Format stats flow-based reporting list of reporting methods
Mode Global Config

Example: The following shows examples of the command.
(FASTPATH Routing) (Config)# stats flow-based reporting console email syslog
(FASTPATH Routing) (Config)# stats flow-based reporting email syslog
(FASTPATH Routing) (Config)# stats flow-based reporting none

3.21.4 stats group
This command applies the group specified on an interface or interface-range.

Format stats group <group id | name>
Mode Interface Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group id</td>
<td>The unique identifier for the group.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the group.</td>
</tr>
</tbody>
</table>

Example: The following shows examples of the command.
(FASTPATH Routing) (Interface 0/1-0/10)# stats group 1
(FASTPATH Routing) (Interface 0/1-0/10)# stats group 2

3.21.4.1 no stats group
This command deletes the interface or interface-range from the group specified.

Format no stats group <group id | name>
Mode Interface Config

Example: The following shows examples of the command.
(FASTPATH Routing) (Interface 0/1-0/10)# no stats group 1
(FASTPATH Routing) (Interface 0/1-0/10)# no stats group 2
3.21.5 stats flow-based

This command applies the flow-based rule specified by the ID on an interface or interface-range.

**Format**

```
stats flow-based <rule-id>
```

**Mode**

Interface Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule-id</td>
<td>The unique identifier for the flow-based rule.</td>
</tr>
</tbody>
</table>

**Example:** The following shows examples of the command.

(FASTPATH Routing) (Interface 0/1-0/10)# stats flow-based 1
(FASTPATH Routing) (Interface 0/1-0/10)# stats flow-based 2

3.21.5.1 no stats flow-based

This command deletes the interface or interface-range from the flow-based rule specified.

**Format**

```
no stats flow-based <rule-id>
```

**Mode**

Interface Config

**Example:** The following shows examples of the command.

(FASTPATH Routing) (Interface 0/1-0/10)# no stats flow-based 1
(FASTPATH Routing) (Interface 0/1-0/10)# no stats flow-based 2

3.21.6 show stats group

This command displays the configured time range and the interface list for the group specified and shows collected statistics for the specified time-range name on the interface list after the time-range expiry.

**Format**

```
show stats group <group id | name>
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group id</td>
<td>The unique identifier for the group.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the group.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show stats group received

Group: received
Time Range: test
Interface List
---------------------
0/2, 0/4, lag 1

<table>
<thead>
<tr>
<th>Counter ID</th>
<th>Interface</th>
<th>Counter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Total</td>
<td>0/2</td>
<td>951600</td>
</tr>
<tr>
<td>Rx Total</td>
<td>0/4</td>
<td>304512</td>
</tr>
<tr>
<td>Rx Total</td>
<td>lag 1</td>
<td>0</td>
</tr>
<tr>
<td>Rx 64</td>
<td>0/2</td>
<td>0</td>
</tr>
<tr>
<td>Rx 64</td>
<td>0/4</td>
<td>4758</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(FASTPATH Routing) #show stats group port-utilization

Group: port-utilization
Time Range: test
Interface List
----------------
0/2, 0/4, lag 1
Interface Utilization (%)
----------------
0/2 0
0/4 0
lag 1 0

3.21.7 show stats flow-based

This command displays the configured time range, flow-based rule parameters, and the interface list for the flow specified.

Format

show stats flow-based rule-id|all

Mode

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule-id</td>
<td>The unique identifier for the flow-based rule.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show stats flow-based all

Flow based rule Id............................ 1
Time Range.................................... test
Source IP.................................... 1.1.1.1
Source MAC.................................. 1234
Source TCP Port............................. 123
Source UDP Port............................. 123
Destination IP.............................. 2.2.2.2
Destination MAC............................. 1234
Destination TCP Port....................... 123
Destination UDP Port....................... 123
Interface List
----------------
0/1 - 0/2

Interface Hit Count
----------------
0/1 100
0/2 0

Flow based rule Id............................ 2
Time Range.................................... test
Source IP.................................... 1.1.1.1
Source TCP Port............................. 123
Example: The following shows example CLI display output for the command.

(FASTPATH Routing) #show stats flow-based 2

Flow based rule Id............................  2
Time Range.................................... test
Source IP...................................... 1.1.1.1
Source TCP Port................................ 123
Source UDP Port................................ 123
Destination IP.................................. 2.2.2.2
Destination TCP Port........................... 123
Destination UDP Port........................... 123

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

(FASTPATH Routing) #show stats flow-based 2

Flow based rule Id............................  2
Time Range.................................... test
Source IP...................................... 1.1.1.1
Source TCP Port................................ 123
Source UDP Port................................ 123
Destination IP.................................. 2.2.2.2
Destination TCP Port........................... 123
Destination UDP Port........................... 123

3.22 Precision Time Protocol (IEEE 1588) Commands

IEEE 1588, also known as precision time protocol (PTP), enables precise synchronization of clocks (with a sub-microsecond accuracy) across a packet-based network. It enables systems of different precision, resolution and stability to synchronize to a grandmaster clock through an exchange of packets across the network.

Typical applications for this protocol include industrial automation, mobile cellular backhaul, financial trading, data centers, and power utility systems.

3.22.1 ptp enable

Use this command to globally enable PTP.

Default Disabled
Format ptp enable
Mode Global Config
3.22.1  **no ptp enable**

Use this command to globally set PTP to the default value.

**Format**   
no ptp enable

**Mode**   
Global Config

3.22.2  **ptp clock boundary domain**

This command configures the boundary clock domain number and enters the clock configuration mode.

**Default**   
Domain: 0
Hybrid mode: Disabled.

**Format**   
ptp clock boundary domain *domain*

**Mode**   
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>The PTP domain number. The range for the domain value is 0–255 for a standard clock and 24–43 for a G.8275.1 telecom phase profile.</td>
</tr>
<tr>
<td>hybrid</td>
<td>Enable PTP hybrid mode.</td>
</tr>
</tbody>
</table>

3.22.2.1  **no ptp clock boundary**

Use this command to reset the clock to the default PTP values. All PTP port configurations associated with the clock will be removed.

**Format**   
no ptp clock boundary

**Mode**   
Global Config

3.22.3  **profile telecom g.8275.1**

This command configures the clock to use the Telecom Phase profile, G.8275.1. This command has a dependency on the `ptp clock boundary domain` command. The domain number configured by the `ptp clock boundary domain` command (see 3.22.2 ptp clock boundary domain) needs to be compliant with G.8275.1. Additionally, if any port configuration exists, it must comply with G.8275.1 (L2 multicast configuration with no user-configured message intervals).

**Default**   
NA

**Format**   
profile telecom g.8275.1

**Mode**   
PTP Clock Config

3.22.3.1  **no profile telecom g.8275.1**

This command removes the G.8275.1 profile configuration.

**Format**   
no profile telecom g.8275.1

**Mode**   
PTP Clock Config
3.22.4 priority1
This command configures the priority1 value of the clock. This value is utilized in the best master clock selection algorithm. Lower values have higher precedence. The range for priority1 is 0–255. When the G.8275.1 telecom phase profile is used, this configuration parameter is not used.

Default 128
Format priority1 priority
Mode PTP Clock Config

3.22.4.1 no priority1
This command resets the priority1 of the clock to the default value.

Format no priority1
Mode PTP Clock Config

3.22.5 priority2
This command configures the priority2 value of the clock. The priority2 value is used as one of the tie-breakers while comparing two otherwise equally qualified clocks. Lower values have a higher precedence. The range for priority2 is 0–255.

Default 128
Format priority2 priority
Mode PTP Clock Config

3.22.5.1 no priority2
This command configures the priority2 value of the clock to default.

Format no priority2
Mode PTP Clock Config

3.22.6 local-priority
This command configures the clock's local priority that will be used in the alternate best master clock algorithm (BMCA) used in G.8275.1 profile.

Default 128
Format local-priority value
Mode PTP Clock Config
3.22.6.1 no local-priority
This command resets the local priority of the clock to default.

Format     no local-priority
Mode       PTP Clock Config

3.22.7 clock-port
This command creates a PTP clock port and execution enters the PTP Port Config mode. The optional parameter, master or slave when specified, indicates the role of the PTP port. By default, a standard PTP port is created.

Default    PTP port role: Standard.
Format     clock-port name [{master | slave}]
Mode       PTP Clock Config

3.22.7.1 no clock-port
This command deletes the PTP clock port.

Format     no clock-port name
Mode       PTP Clock Config

3.22.8 transport ethernet multicast vlan
This command configures the PTP port to use PTPoL2 multicast. The vlan_id parameter specifies the VLAN on which PTP packets will be exchanged for this PTP port.

Default    NA
Format     transport ethernet multicast vlan vlan_id
Mode       PTP Port Config

3.22.8.1 no transport
This command unconfigures the PTP port.

Format     no transport
Mode       PTP Port Config

3.22.9 announce interval
This command configures the PTP announce message interval, which is the interval between two consecutive announce messages sent out on this port. Note that the interval is expressed as a logarithmic value. The range of log_seconds is –2 to 4. A value of 4 means that one message is sent every 2^4 (16) seconds. This command cannot be issued when the clock is in G.8275.1 mode.

Default    1 (One announce message every two seconds)
Format     announce interval log_seconds
Mode       PTP Port Config
3.22.9.1 no announce interval

This command sets the announce interval on the port to default.

**Format**

no announce interval

**Mode**

PTP Port Config

3.22.10 announce timeout

This command configures the PTP announce receipt timeout on the interface. This timeout value configures the number of PTP intervals before a timeout occurs (due to non-receipt of announce messages). The range of `value` is 2–10.

**Default**

3

**Format**

announce timeout value

**Mode**

PTP Port Config

3.22.10.1 no announce timeout

This command sets the announce receipt timeout on the port to default.

**Format**

no announce timeout

**Mode**

PTP Port Config

3.22.11 delay-req interval

This command configures the PTP delay request interval for the port, which is the minimum duration between successive delay requests allowed on the port. The `value` range is –7 to 5. This command cannot be issued when the clock is in G.8275.1 mode.

**Default**

–5

**Format**

delay-req interval value

**Mode**

PTP Port Config

3.22.11.1 no delay-req interval

This command sets the minimum delay request interval on the port to default.

**Format**

no delay-req interval

**Mode**

PTP Port Config

3.22.12 sync interval

This command configures the PTP synchronization message interval, which is the interval between two consecutive synchronization messages sent out on this port. Note that the interval is expressed as a logarithmic value. The range for `log_seconds` is –7 to 1. A value of 1 means one message is sent every $2^1$ (2) seconds. This command cannot be issued when the clock is in G.8275.1 mode.

**Default**

–5

**Format**

sync interval log_seconds

**Mode**

PTP Port Config
### 3.22.12 no sync interval
This command sets the sync interval on the port to default.

**Format**
```
no sync interval
```

**Mode**
PTP Port Config

### 3.22.13 local-priority
This command configures the port’s local priority that will be used in the alternate BMCA algorithm used in the G.8275.1 profile.

**Default**
128

**Format**
```
local-priority value
```

**Mode**
PTP Port Config

### 3.22.13.1 no local-priority
This command resets the local priority of port to default.

**Format**
```
no local-priority
```

**Mode**
PTP Port Config

### 3.22.14 ptp udp debug
This command enables time-of-day processor (ToP) UDP logging. UDP packets are sent with the following parameters:

- **DMAC**: Broadcast
- **SMAC**: 0x00, 0x10, 0x18, 0x00, 0x00, 0x01
- **UDP port num**: 0x4455
- **Src IP**: 192.168.0.90
- **Destination IP**: 255.255.255.255
- **TTL**: 1
- **VLAN**: 1

**Default**
Disabled

**Format**
```
ptp udp debug
```

**Mode**
Privileged Exec

### 3.22.14.1 no ptp udp debug
Use this command to set the ToP UDP logging to the default value.

**Format**
```
no ptp udp debug
```

**Mode**
Privileged Exec
3.22.15  show ptp time
This command displays the current PTP time.

**Format**  show ptp time
**Mode**  Privileged Exec

*Example:* The following command shows the command output:

(Broadcom FASTPATH Routing) #show ptp time
Seconds........................................ 1
Nanoseconds.................................... 112611328

3.22.16  show ptp
This command displays PTP global config.

**Format**  show ptp
**Mode**  Privileged Exec

*Example:* The following command shows the command output:

(Broadcom FASTPATH Routing) #show ptp
PTP Mode.................................... Enabled
Domain Number................................ 1
Priority1..................................... 128
Priority2..................................... 128
Mode.......................................... Normal
Telecom profile(g.8275.1)..................... Disabled

3.22.17  show ptp clock running domain
This command displays PTP clock data.

**Format**  show ptp clock running domain domain-number
**Mode**  Privileged Exec

*Example:* The following command shows the command output:

(Broadcom FASTPATH Routing) #show ptp clock running domain 25
PTP Boundary Clock [Domain 25]

<table>
<thead>
<tr>
<th>State</th>
<th>Ports</th>
<th>Packets Sent</th>
<th>Packets Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquiring  lock</td>
<td>32</td>
<td>1409319</td>
<td>0</td>
</tr>
</tbody>
</table>

PORT SUMMARY

<table>
<thead>
<tr>
<th>Name</th>
<th>Mode</th>
<th>Role</th>
<th>Transport</th>
<th>State</th>
<th>PTP Port</th>
<th>Master Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td>Multicast</td>
<td>Standard Ethernet</td>
<td>Master</td>
<td>1</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
3.22.18  show ptp clock dataset current
This commands displays the clock current dataset.

Format  show ptp clock dataset current
Mode    Privileged Exec

Example: The following command shows the command output:
(Broadcom FASTPATH Routing) #show ptp clock dataset current

CLOCK [Boundary Clock, domain 25]
Steps Removed........................................... 0
Offset From Master........................................... 0 ns
Mean Path Delay........................................... 0 ns

3.22.19  show ptp clock dataset default
This commands displays the clock default dataset.

Format  show ptp clock dataset default
Mode    Privileged Exec

Example: The following command shows the command output:
(Broadcom FASTPATH Routing) #show ptp clock dataset default

CLOCK [Boundary Clock, domain 25]
Two Step Flag........................................... No
Clock Identity........................................... 00:0a:f7:ff:fe:81:84:f3
Number Of Ports........................................... 32
Priority1........................................... 128
Priority2........................................... 128
Local Priority........................................... 128
Slave only........................................... No

Clock Quality:
Class........................................... 248
Accuracy........................................... 0xfe
Offset (log variance)........................................... 0xffff

3.22.20  show ptp clock dataset parent domain
This commands displays the clock parent dataset.

Format  show ptp clock dataset parent domain domain-number
Mode    Privileged Exec

Example: The following command shows the command output:
(Broadcom FASTPATH Routing) #show ptp clock dataset parent domain 25

CLOCK [Boundary Clock, domain 25]
Parent Stats........................................... No
Observed Parent Offset (log variance)........... 0
Observed Parent Clock Phase Change Rate........... 0
Clock Port Identity........................................... 00:0a:f7:ff:fe:81:84:f3
Port number........................................... 1
Grandmaster Clock:
  Identity.......................... 00:0a:f7:ff:fe:81:84:f3
  Priority 1........................... 128
  Priority 2........................... 128

Grandmaster Clock Quality:
  Class.................................. 248
  Accuracy.............................. 0xfe
  Offset (log variance)................ 0xffff

3.22.21  show ptp clock dataset time-properties domain
This command displays the clock time-properties dataset.

Format show ptp clock dataset time-properties domain domain-number
Mode  Privileged Exec

Example: The following command shows the command output:
(Broadcom FASTPATH Routing) #show ptp clock dataset time-properties domain 1

CLOCK [Boundary Clock, domain 1]
  Current UTC Offset Valid............ FALSE
  Current UTC Offset.................. 34
  Leap 59................................... FALSE
  Leap 61................................... FALSE
  Time Traceable........................ FALSE
  Frequency Traceable................... FALSE
  PTP Timescale........................... FALSE
  Time Source............................ Internal oscillator

3.22.22  show ptp clock dataset domain
This command displays the combined output for show ptp clock dataset parent domain and show ptp clock dataset time-properties.

Format show ptp clock dataset domain domain-number
Mode  Privileged Exec

Example: The following command shows the command output:
(Broadcom FASTPATH Routing) #show ptp clock dataset domain 25

Parent:
  CLOCK [Boundary Clock, domain 25]
  Parent Stats........................... No
  Observed Parent Offset (log variance)........ 0
  Observed Parent Clock Phase Change Rate...... 0
  Clock Port Identity..................... 00:0a:f7:ff:fe:81:84:f3
  Port number........................... 1

Grandmaster Clock:
  Identity............................ 00:0a:f7:ff:fe:81:84:f3
  Priority 1............................ 128
  Priority 2............................ 128

Grandmaster Clock Quality:
  Class.................................. 248
Accuracy................................. 0xfe
Offset (log variance).................. 0xffff

Time Properties:

CLOCK [Boundary Clock, domain 25]

Current UTC Offset Valid.................. FALSE
Current UTC Offset........................ 34
Leap 59..................................... FALSE
Leap 61..................................... FALSE
Time Traceable.............................. FALSE
Frequency Traceable........................ FALSE
PTP Timescale.............................. FALSE
Time Source.................................. Internal Oscillator

3.22.23 show ptp port dataset port

This command displays PTP clock port dataset.

**Format**    show ptp port dataset port name

**Mode**      Privileged Exec

**Example:** The following command shows the command output:
(Broadcom FASTPATH Routing) #show ptp port dataset port port1

PTP Port Dataset:

Port identity:
  Clock identity........................... 00:0a:f7:ff:fe:81:84:f3
  Port number................................ 1

PTP version............................... 2
Port state.................................. Master
Configured Port Type...................... Standard
Delay request interval(log mean)...........
  Announce receipt time out..............
Peer mean path delay......................
  Announce interval(log mean)...........
Sync interval(log mean)....................
Delay Mechanism............................ End to End
Local Priority............................. 128

3.22.24 show platform ptp state

This command displays PTP servo master information.

**Format**    show ptp platform ptp state

**Mode**      Privileged Exec

**Example:** The following command shows the command output:
(Broadcom FASTPATH Routing) #show platform ptp state

FLL State.................................. Acquiring lock
FLL Status Duration........................ 56069(sec)
Forward Flow Weight...................... 0
Forward Flow Transient-Free(900 sec Window).... 0(sec)
Forward Flow Transient-Free(3600 sec Window).... 0(sec)
Forward Flow Transactions Used.............. 0(%)
Forward Flow Oper. Min TDEV............... 0(nsec)
Forward Mafie........................................ 0
Forward Flow Min Cluster Width........... 788491634(nsec)
Forward Flow Mode Width.................. 1(nsec)
Reverse Flow Weight.......................... 0
Reverse Flow Transient-Free(900 sec Window).... 0(sec)
Reverse Flow Transient-Free(3600 sec Window)... 0(sec)
Reverse Flow Transactions Used.............. 0(%)
Reverse Flow Oper. Min TDEV................ 0(nsec)
Reverse Mafie........................................ 0
Reverse Flow Min Cluster Width........... 0(nsec)
Reverse Flow Mode Width.................. 0(nsec)
Frequency Correction.......................... 0(ppb)
Phase Correction............................... 0(ppb)
Output TDEV Estimate......................... 0(nsec)
Output MDEV Estimate.......................... 0(ppb)
Residual Phase Error........................... 0(nsec)
Min. Roundtrip Delay......................... 0(nsec)
Sync Packet Rate............................... 0(pkts/sec)
Delay Packet Rate .............................. 0(pkts/sec)
Forward IPDV % Below Threshold............ 0
Forward Maximum IPDV ........................... 0(usec)
Forward Interpacket Jitter................... 0(usec)
Reverse IPDV % Below Threshold............ 0
Reverse Maximum IPDV ........................... 0(usec)
Reverse Interpacket Jitter................... 0(usec)

**3.22.25  show platform ptp stats**

This command displays PTP statistics.

**Format**        show platform ptp stats

**Mode**          Privileged Exec

**Example:** The following command shows the command output:
(Broadcom FASTPATH Routing) #show platform ptp stats

Statistics for PTP clock 0 :

Packets Received.............................. 0
Packets Transmitted........................... 1414509
Packets Discarded............................. 0

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Packets Received</th>
<th>Packets Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td>168</td>
<td>471672</td>
</tr>
</tbody>
</table>

**3.22.26  show platform ptp**

This command displays the combined output of show platform ptp stats and show platform ptp state commands.

**Format**        show platform ptp

**Mode**          Privileged Exec

**Example:** The following command shows the command output:
(Broadcom FASTPATH Routing) #show platform ptp

Stats:

Statistics for PTP clock 0 :
Packets Received......................... 0
Packets Transmitted...................... 1419123
Packets Discarded....................... 0

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Packets Received</th>
<th>Packets Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1</td>
<td>174</td>
<td>473216</td>
</tr>
</tbody>
</table>

State:

FLL State................................ Acquiring lock
FLL Status Duration..................... 59208(sec)
Forward Flow Weight...................... 0
Forward Flow Transient-Free(900 sec Window)... 0(sec)
Forward Flow Transient-Free(3600 sec Window)... 0(sec)
Forward Flow Transactions Used................ 0(%)  
Forward Flow Oper. Min TDEV..................... 0(nsec)
Forward Maeie................................ 0
Forward Flow Min Cluster Width............ 0(nsec)
Forward Flow Mode Width.................... 0(nsec)
Reverse Flow Weight...................... 0
Reverse Flow Transient-Free(900 sec Window)... 0(sec)
Reverse Flow Transient-Free(3600 sec Window)... 0(sec)
Reverse Flow Transactions Used................ 0(%)  
Reverse Flow Oper. Min TDEV..................... 0(nsec)
Reverse Maeie................................ 0
Reverse Flow Min Cluster Width............ 0(nsec)
Reverse Flow Mode Width.................... 0(nsec)
Frequency Correction..................... 0(ppb)
Phase Correction......................... 0(ppb)
Output TDEV Estimate...................... 0(nsec)
Output MDEV Estimate...................... 0(ppb)
Residual Phase Error...................... 0(nsec)
Min. Roundtrip Delay...................... 0(nsec)
Sync Packet Rate........................... 0(pkts/sec)
Delay Packet Rate......................... 0(pkts/sec)
Forward IPDV % Below Threshold............ 0
Forward Maximum IPDV........................ 0(usec)
Forward Interpacket Jitter............... 0(usec)
Reverse IPDV % Below Threshold............ 0
Reverse Maximum IPDV........................ 0(usec)
Reverse Interpacket Jitter............... 0(usec)

3.22.27 show platform ptp stats detailed

This command displays PTP statistics in detail per port. The statistics are reset on read, and hence indicate incremental values since the last invocation of this command.

Format show platform ptp stats detailed port-name
Mode Privileged Exec

Example: The following command shows the command output:

Router# show platform ptp stats detailed slave

Statistics for peer 0:
Protocol address ......................... 10.10.10.10
Announces Sent .......................... 0
Announces Rcvd .......................... 297
Syncs Sent .............................. 0
Syncs Rcvd .............................. 37925
Follow Ups Sent .......................... 0
Follow Ups Rcvd ............................ 37925
Delay ReqS Sent ............................ 37404
Delay ReqS Rcvd ............................ 0
Delay Resps Sent ............................ 0
Delay Resps Rcvd ............................ 37404

3.22.28  show ptp master

This command displays PTP master information.

**Format**  
show ptp master

**Mode**  
Privileged Exec

*Example:* The following command shows the command output:

```
Router#show ptp master
```

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Index</th>
<th>Master protocol address</th>
<th>Announce Interval</th>
<th>Sync Interval</th>
<th>Delay Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLAVE</td>
<td>1</td>
<td>00:90:56:26:46:1e</td>
<td>1</td>
<td>-6</td>
<td>-6</td>
</tr>
</tbody>
</table>

3.22.29  show ptp peers

This command displays PTP peer information for the system. When port name is specified, it displays the PTP peers on a port.

**Format**  
show ptp peers

**Mode**  
Privileged Exec

*Example:*

```
Router#show ptp peers
```

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Index</th>
<th>Master protocol address</th>
<th>Announce Interval</th>
<th>Sync Interval</th>
<th>Delay Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>MASTER</td>
<td>1</td>
<td>00:90:56:26:46:1e</td>
<td>1</td>
<td>-6</td>
<td>-6</td>
</tr>
<tr>
<td>MASTER1</td>
<td>2</td>
<td>00:90:56:26:46:10</td>
<td>1</td>
<td>-6</td>
<td>-6</td>
</tr>
</tbody>
</table>
3.23 Power Over Ethernet Commands

This section describes the commands used to configure and monitor Power Over Ethernet (PoE). PoE allows IP telephones, wireless LAN access points, and other appliances to receive power as well as data over existing LAN cabling without modifying the existing Ethernet infrastructure. PoE is only available on switches that contain a PoE controller.

PoE implements the PoE+ specification (IEEE 802.3at) for power sourcing equipment (PSE). IEEE 802.3at allows power to be supplied to Class 4 PD devices that require power greater than 15.4 Watts and up to 34.2 Watts. This allows the PoE+ enabled network switches and routers to be used for deployment with devices that require more power than the 802.3AF specification allows. PoE+ 802.3at is compatible with 802.1AF.

**Flexible Power Management**

PoE provides power management that supports power reservation, power prioritization and power limiting. The operator can assign a priority to each PoE port. When the power budget of the PoE switch has been exhausted, the higher priority ports are given preference over the lower priority ports. Lower priority ports are forcibly stopped to supply power in order to provide power to higher priority ports.

The static power management feature allows operators to reserve a guaranteed amount of power for a PoE port. This is useful for powering up devices which draw variable amounts of power and provide them an assured power range within which to operate. Class-based power management allocates power at class limits as opposed to user defined limits.

In the Dynamic Power management feature, power is not reserved for a given port at any point of time. The power available with the PoE switch is calculated by subtracting the instantaneous power drawn by all the ports from the maximum available power. Thus, more ports can be powered at the same time. This feature is useful to efficiently power up more devices when the available power with the PoE switch is limited.

PoE also provides a global usage threshold feature in order to limit the PoE switch from reaching an overload condition. The operator can specify the limit as a percentage of the maximum power.

---

**POE commands are only available on PoE enabled systems.**

---

**POE commands are only applicable to copper ports.**

---

### 3.23.1 poe

Use this command to enable/disable PoE admin mode. If enabled, all ports (Interface Config mode) or the selected port (Interface Config mode) are capable of delivering power to a PD. If disabled, none of the ports can deliver power to a PD.

---

**POE admin mode does not impact the functionality of the Ethernet port itself; disabling admin mode only turns off the capability to deliver power.**

---

**NOTICE**

This command is only available on platforms with a Broadcom PoE controller.

---

**Default**

Enabled

**Format**

poe

**Mode**

- Global Configuration
- Interface Configuration
3.23.2 poe detection

Use this command to set the detection mode. Detection mode is used to set the type of devices that will be allowed for powering up. You can configure the PoE controller to detect only IEEE standard devices or pre-IEEE legacy devices (which were pre-standard). Use the no form of the command to bring detection mode back to the default setting of auto.

This command is only available on platforms with a Broadcom PoE controller.

<table>
<thead>
<tr>
<th>Default</th>
<th>auto</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>poe detection {auto</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Detects both standard and non-standard devices.</td>
</tr>
<tr>
<td>ieee</td>
<td>Detects IEEE standard devices.</td>
</tr>
<tr>
<td>pre-ieee</td>
<td>Detects legacy devices.</td>
</tr>
</tbody>
</table>

3.23.3 poe high-power

Use this command to enable high power mode for all ports in all units (Global Configuration) or for a specific unit (Interface Configuration mode). In high power mode, the switch negotiates the power budget with the powered device (PD). The maximum power a POE port is capable of delivering is 32W in dot3at mode and 60W in upoe mode.

<table>
<thead>
<tr>
<th>Default</th>
<th>Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>poe high-power {dot3at</td>
</tr>
<tr>
<td>Mode</td>
<td>• Global Configuration</td>
</tr>
<tr>
<td></td>
<td>• Interface Configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot3at</td>
<td>High power device with LLDP support</td>
</tr>
<tr>
<td>legacy</td>
<td>Powered device with a high-inrush current</td>
</tr>
<tr>
<td>pre-dot3at</td>
<td>Powered device without LLDP support</td>
</tr>
<tr>
<td>upoe</td>
<td>Forces power to be delivered using four pairs of the cable. This option is available only on non-Broadcom PoE controllers.</td>
</tr>
</tbody>
</table>

3.23.3.1 no poe high-power

Disables high power mode.

<table>
<thead>
<tr>
<th>Format</th>
<th>no poe high-power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>• Global Configuration</td>
</tr>
<tr>
<td></td>
<td>• Interface Configuration</td>
</tr>
</tbody>
</table>
3.23.4  poe power limit

Use this command to configure the type of power limit for all ports in all units (Global Configuration) or a specified port (Interface Configuration).

**Default**  User-defined value

**Format**  
```
poe power limit {none | value | class-based}
```

**Mode**
- Global Configuration
- Interface Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>There is no power limit.</td>
</tr>
<tr>
<td>value</td>
<td>A user-defined power limit from 3000 mW to 32000 mW power per port.</td>
</tr>
<tr>
<td>class-based</td>
<td>The power limit is class-based.</td>
</tr>
</tbody>
</table>

3.23.4.1  no poe power limit

Use this command to set the power limit type to the default.

**Default**  User-defined value

**Format**  
```
no poe power limit
```

**Mode**
- Global Configuration
- Interface Configuration

3.23.5  poe power management

Use this command to set up the power management type.

**Default**  Dynamic

**Format**  
```
poe power management {unit/slot/port | all} {dynamic | static}
```

**Mode**  Global Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit</td>
<td>Configures power management for an individual port.</td>
</tr>
<tr>
<td>all</td>
<td>Configures power management for all ports.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Power management is done by the POE controller and the maximum power for a port is not reserved for each port.</td>
</tr>
<tr>
<td>static</td>
<td>Power management is done by the POE controller and maximum power for a port is reserved.</td>
</tr>
</tbody>
</table>
3.23.5.1 no poe power management
Use this command to set the management mode to the default.

Format: 
Mode: Global Configuration

3.23.6 poe priority
Use this command to configure the port priority level for the delivery of power to an attached device. The switch may not be able to supply power to all connected devices, so the port priority is used to determine which ports will supply power if adequate power capacity is not available for all enabled ports. For ports that have the same priority level the lower-numbered port has higher priority.

For a system delivering peak power to a certain number of devices, if a new device is attached to a high-priority port, power to a low-priority port is shut down and the new device is powered up.

Default: Low
Format: 
Mode: Interface Configuration

**NOTICE** Medium is only available on non-Broadcom PoE controllers.

3.23.6.1 no poe priority
Use this command to return the port priority level to the default value.

Default: Low
Format: 
Mode: Global Configuration, Interface Configuration

3.23.7 poe reset
Use this command to reset all ports.

Default: Disable
Format: 
Mode: Global Configuration

3.23.8 poe timer schedule
Use this command to attach a timer schedule to a port. It is useful to allow ports to automatically be configured to deliver power based on time intervals, etc. For example, if a user wants to allow ports to deliver power only on weekdays and not on weekends, a timer schedule can be configured and attached to the port such that PoE is disabled on the weekends automatically.

**NOTICE** This command is only available on platforms with a Broadcom PoE controller.
3.23.9   poe traps

Use this command to enable/disable traps that indicate changes in the PoE status for the port.

Default        Enable
Format          poe traps
Mode            Global Configuration

3.23.10   poe usagethreshold

Use this command to configure the system power usage threshold level at which a trap is generated. The threshold is configured as a percentage of the total available power.

Default        90%
Format          poe usagethreshold {unit | all} 1-99
Mode            Global Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit</td>
<td>Sets the threshold for the unit.</td>
</tr>
<tr>
<td>all</td>
<td>Sets the threshold for all units.</td>
</tr>
<tr>
<td>1-99</td>
<td>The power threshold at which a trap is generated. The range is 1-99%.</td>
</tr>
</tbody>
</table>
3.23.10.1 no poe usagethreshold
Use this command to set the threshold to the default value.

Format  no poe usagethreshold
Mode    Global Configuration

3.23.11 show poe
Use this command to display the current POE configuration and status information for all ports.

Format  show poe
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Version</td>
<td>Displays the firmware version on the controller. This cannot be changed/upgraded.</td>
</tr>
<tr>
<td>PSE Main Operational Status</td>
<td>The operational status of the PSE.</td>
</tr>
<tr>
<td>Total Power Available</td>
<td>The total power budget</td>
</tr>
<tr>
<td>Threshold Power</td>
<td>The total power minus the guard band. If usage goes above this value, new ports are not powered up.</td>
</tr>
<tr>
<td>Total Power Consumed</td>
<td>Total power delivered by all ports.</td>
</tr>
<tr>
<td>Usage Threshold</td>
<td>Threshold configured by the user. This is used for Guard band calculation.</td>
</tr>
<tr>
<td>Power Management Mode</td>
<td>The current power management mode: Dynamic or Static.</td>
</tr>
<tr>
<td>Traps</td>
<td>If PoE traps are enabled or disabled.</td>
</tr>
</tbody>
</table>

Example:
(Switching) #show poe
Firmware Version......................... 1.3.0.7
PSE Main Operational Status.............. OFF
Total Power Available..................... 900 Watts
Threshold Power.......................... 459 W
Total Power Consumed...................... 0
Usage Threshold........................... 90
Power Management Mode.................... Dynamic
Traps..................................... Enable

3.23.12 show poe mpsm
Use this command to display the current MPSM and Power Bank values. If a slot is selected, only the MPSM and Power Bank Values for that slot are displayed.

Format  show poe mpsm [slot]
Mode    Privileged EXEC

This command is only available on non-Broadcom PoE controllers.
**Example:**

(Switching)# show poe mpism

Current Active MPSM = 1

<table>
<thead>
<tr>
<th>Slot</th>
<th>Power Bank Value (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>580</td>
</tr>
<tr>
<td>2</td>
<td>610</td>
</tr>
<tr>
<td>3</td>
<td>550</td>
</tr>
</tbody>
</table>

(Switching) show poe mpism 2

Slot = 2

Current Active MPSM = 1

<table>
<thead>
<tr>
<th>MPSM Number:</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Bank Value (W):</td>
<td>260</td>
<td>610</td>
<td>1080</td>
<td>1430</td>
<td>1780</td>
<td>2130</td>
<td>2480</td>
<td>2830</td>
</tr>
</tbody>
</table>

### 3.23.13 show poe port configuration

Use this command to display POE port configuration information for individual ports or all ports.

**Format**

show poe port configuration { all | unit/slot/port }

**Mode**

Privileged EXEC

**Example:**

(Switching) #show poe port configuration 0/1

<table>
<thead>
<tr>
<th>Intf</th>
<th>Admin Mode</th>
<th>Priority</th>
<th>Power Limit Type</th>
<th>High Power Limit Type</th>
<th>Detection Type</th>
<th>Timer Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Enable</td>
<td>Low</td>
<td>User Defined</td>
<td>UPOE</td>
<td>auto</td>
<td>None</td>
</tr>
</tbody>
</table>

### 3.23.14 show poe port info

Use this command to display PoE port information.

**Format**

show poe port info { all | unit/slot/port }

**Mode**

Privileged EXEC

**Example:**

(Switching) #show poe port info all

<table>
<thead>
<tr>
<th>Intf</th>
<th>High Power (mW)</th>
<th>Max Power (mW)</th>
<th>Class</th>
<th>Power Limit (mW)</th>
<th>Output Current (mA)</th>
<th>Output Voltage (V)</th>
<th>Status</th>
<th>Fault Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/8/1</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/2</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/3</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/4</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/5</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/6</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/7</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/8</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/9</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/10</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>2/8/11</td>
<td>Yes</td>
<td>32000</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Status</td>
<td>Link Speed</td>
<td>Link Delay</td>
<td>Path Delay</td>
<td>Oper Status</td>
<td>Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
<td>-------------</td>
<td>-------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/0/12</td>
<td>Yes</td>
<td>32000</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/0/13</td>
<td>Yes</td>
<td>32000</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/0/14</td>
<td>Yes</td>
<td>32000</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/0/15</td>
<td>Yes</td>
<td>32000</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/0/16</td>
<td>Yes</td>
<td>32000</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/0/17</td>
<td>Yes</td>
<td>32000</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/0/18</td>
<td>Yes</td>
<td>32000</td>
<td>0</td>
<td>0</td>
<td>Disabled</td>
<td>No Error</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4 / Switching Commands

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

The Switching Commands chapter includes the following sections:

- “Port Configuration Commands” on page 290
- “Spanning Tree Protocol Commands” on page 298
- “Loop Protection Commands” on page 322
- “VLAN Commands” on page 325
- “Double VLAN Commands” on page 336
- “Private VLAN Commands” on page 339
- “Switch Ports” on page 341
- “Voice VLAN Commands” on page 344
- “Provisioning (IEEE 802.1p) Commands” on page 346
- “Asymmetrical Flow Control” on page 347
- “Protected Ports Commands” on page 348
- “GARP Commands” on page 350
- “GVRP Commands” on page 351
- “GMRP Commands” on page 353
- “Port-Based Network Access Control Commands” on page 355
- “802.1X Supplicant Commands” on page 371
- “Storm-Control Commands” on page 374
- “Link Dependency Commands” on page 382
- “Link Local Protocol Filtering Commands” on page 384
- “MVR Commands” on page 385
- “Port-Channel/LAG (802.3ad) Commands” on page 389
- “VPC Commands” on page 407
- “Port Mirroring Commands” on page 418
- “Static MAC Filtering Commands” on page 424
- “DHCP L2 Relay Agent Commands” on page 427
- “DHCP Client Commands” on page 433
- “DHCP Snooping Configuration Commands” on page 435
- “Dynamic ARP Inspection Commands” on page 443
- “IGMP Snooping Configuration Commands” on page 449
- “IGMP Snooping Querier Commands” on page 457
- “MLD Snooping Commands” on page 460
- “MLD Snooping Querier Commands” on page 468
- “Port Security Commands” on page 470
- “LLDP (802.1AB) Commands” on page 474
- “LLDP-MED Commands” on page 481
- “Denial of Service Commands” on page 488
- “MAC Database Commands” on page 498
- “ISDP Commands” on page 499
- “Interface Error Disable and Auto Recovery” on page 505
- “Port Bridging Commands” on page 508

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

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

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

4.1.1 interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port). You can also specify a range of ports to configure at the same time by specifying the starting slot/port and ending slot/port, separated by a hyphen.

Format: \texttt{interface \{slot/port | slot/port(startrange)-slot/port(endrange)\}}

Mode: Global Config

\textbf{Example}: The following example enters Interface Config mode for port 0/1:

\begin{verbatim}
(switch) #configure
(switch) (config)#interface 0/1
(switch) (interface 0/1)#
\end{verbatim}

\textbf{Example}: The following example enters Interface Config mode for ports 0/1 through 0/4:

\begin{verbatim}
(switch) #configure
(switch) (config)#interface 0/1-0/4
(switch) (interface 0/1-0/4)#
\end{verbatim}

4.1.2 auto-negotiate

This command enables automatic negotiation on a port or range of ports.

Default: enabled

\textbf{Format}: \texttt{auto-negotiate}

Mode: Interface Config

4.1.2.1 no auto-negotiate

This command disables automatic negotiation on a port.

\textbf{Format}: \texttt{no auto-negotiate}

Mode: Interface Config

\textbf{Notice}: Automatic sensing is disabled when automatic negotiation is disabled.

4.1.3 auto-negotiate all

This command enables automatic negotiation on all ports.

Default: enabled

\textbf{Format}: \texttt{auto-negotiate all}

Mode: Global Config
4.1.3.1  **no auto-negotiate all**
This command disables automatic negotiation on all ports.

**Format**  
no auto-negotiate all

**Mode**  
Global Config

4.1.4  **description**
Use this command to create an alpha-numeric description of an interface or range of interfaces.

**Format**  
description description

**Mode**  
Interface Config

4.1.5  **media-type**
Use this command to change between fiber and copper mode on the Combo port.

- **Combo Port:** A port or an interface that can operate in either copper or in fiber mode.
- **Copper and Fiber port:** A port that uses copper a medium for communication (for example, RJ45 ports). A fiber port uses the fiber optics as a medium for communication (for example, example SFP ports).

**Default**  
Auto-select, SFP preferred

**Format**  
media-type {auto-select | rj45 | sfp}

**Mode**  
Interface Config

The following modes are supported by the `media-type` command.

- **Auto-select, SFP preferred:** The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the fiber link takes precedence and the fiber link is up.
- **Auto-select, RJ45 preferred:** The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the copper link takes precedence and the copper link is up.
- **SFP:** Only the fiber medium works. The copper medium is always down.
- **RJ45:** Only the copper medium works. The fiber medium is always down.

4.1.5.1  **no media-type**
Use this command to revert the `media-type` configuration and configure the default value on the interface.

**Format**  
no media-type

**Mode**  
Interface Config

4.1.6  **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.

---

**NOTICE**  
To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see "ip mtu" on page 521.
4.1.6.1 no mtu
This command sets the default MTU size (in bytes) for the interface.

<table>
<thead>
<tr>
<th>Default</th>
<th>1518 (untagged)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>mtu 1518-12288</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

4.1.7 shutdown
This command disables a port or range of ports.

- **Default**: enabled
- **Format**: shutdown
- **Mode**: Interface Config

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

4.1.7.1 no shutdown
This command enables a port.

- **Format**: no shutdown
- **Mode**: Interface Config

4.1.8 shutdown all
This command disables all ports.

- **Default**: enabled
- **Format**: shutdown all
- **Mode**: Global Config

You can use the `shutdown all` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.
4.1.8.1   no shutdown all
This command enables all ports.

Format       no shutdown all
Mode         Global Config

4.1.9         speed
Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. The
duplex parameter allows you to set the advertised speed for both half as well as full duplex mode.
Use the auto keyword to enable auto-negotiation on the port. Use the command without the auto keyword to ensure
auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is
disabled, the speed and duplex mode must be set.

Default      Auto-negotiation is enabled.
Format       speed auto {10|100|1000|10G} [10|100|1000|10G] [half-duplex|full-duplex]
             speed {10|100|1000|10G} {half-duplex|full-duplex}.
Mode         Interface Config

4.1.10        speed all
This command sets the speed and duplex setting for all interfaces if auto-negotiation is disabled. If auto-negotiation is
enabled, an error message is returned. Use the no auto-negotiate command to disable.

Default      Auto-negotiation is enabled. Adv. is 10h, 10f, 100h, 100f, 1000f.
Format       speed all {100 | 10} {half-duplex | full-duplex}
Mode         Global Config

4.1.11        show interface media-type
Use this command to display the media-type configuration of the interface.

Format       show interface media-type
Mode         Privileged EXEC

The following information is displayed for the command.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Interface in slot/port format.</td>
</tr>
<tr>
<td>Configured Media Type</td>
<td>The media type for the interface.</td>
</tr>
<tr>
<td></td>
<td>auto-select—The media type is automatically selected. The preferred media type is displayed.</td>
</tr>
<tr>
<td></td>
<td>RJ45—RJ45</td>
</tr>
<tr>
<td></td>
<td>SFP—SFP</td>
</tr>
<tr>
<td>Active</td>
<td>Displays the current operational state of the combo port.</td>
</tr>
</tbody>
</table>

**Example:** The following command shows the command output:
(Routing) #show interface media-type

<table>
<thead>
<tr>
<th>Port</th>
<th>Configured Media Type</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/21</td>
<td>SFP</td>
<td>RJ45</td>
</tr>
</tbody>
</table>
4.1.12 show port

This command displays port information.

**Format**  
`show port {intf-range | all}`

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
</tbody>
</table>
| Type      | If not blank, this field indicates that this port is a special type of port. The possible values are:  
• Mirror — this port is a monitoring port. For more information, see "Port Mirroring Commands" on page 418.  
• PC Mbr— this port is a member of a port-channel (LAG).  
• Probe — this port is a probe port. |
| Admin Mode| The Port control administration state. The port must be enabled in order for it to be allowed into the network. May be enabled or disabled. The factory default is enabled. |
| Physical Mode| The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto. |
| Physical Status| The port speed and duplex mode. |
| Link Status| The Link is up or down. |
| Link Trap| This object determines whether or not to send a trap when link status changes. The factory default is enabled. |
| LACP Mode| LACP is enabled or disabled on this port. |

**Example:** The following command shows an example of the command output for all ports.

(Routing) #show port all

<table>
<thead>
<tr>
<th>Intf</th>
<th>Type</th>
<th>Admin Mode</th>
<th>Physical Mode</th>
<th>Physical Status</th>
<th>Link Status</th>
<th>Link Trap</th>
<th>LACP Mode</th>
<th>Actor</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
<td>long</td>
</tr>
<tr>
<td>0/2</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
<td>long</td>
</tr>
<tr>
<td>0/3</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
<td>long</td>
</tr>
<tr>
<td>0/4</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
<td>long</td>
</tr>
<tr>
<td>0/5</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
<td>long</td>
</tr>
<tr>
<td>0/6</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
<td>long</td>
</tr>
<tr>
<td>0/7</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
<td>long</td>
</tr>
<tr>
<td>0/8</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td></td>
<td>long</td>
</tr>
<tr>
<td>1/1</td>
<td>Enable</td>
<td>Auto</td>
<td>Down</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/2</td>
<td>Enable</td>
<td>Auto</td>
<td>Down</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/3</td>
<td>Enable</td>
<td>Auto</td>
<td>Down</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/4</td>
<td>Enable</td>
<td>Auto</td>
<td>Down</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/5</td>
<td>Enable</td>
<td>Auto</td>
<td>Down</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/6</td>
<td>Enable</td>
<td>Auto</td>
<td>Down</td>
<td>Disable</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example: The following command shows an example of the command output for a range of ports.

(Routing) # show port 0/1-6

<table>
<thead>
<tr>
<th>Intf</th>
<th>Type</th>
<th>Admin Mode</th>
<th>Link Status</th>
<th>Link Trap</th>
<th>LACP Actor</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable long</td>
</tr>
<tr>
<td>0/2</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable long</td>
</tr>
<tr>
<td>0/3</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable long</td>
</tr>
<tr>
<td>0/4</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable long</td>
</tr>
<tr>
<td>0/5</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable long</td>
</tr>
<tr>
<td>0/6</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable long</td>
</tr>
<tr>
<td>0/7</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable long</td>
</tr>
<tr>
<td>0/8</td>
<td>Enable</td>
<td>Auto</td>
<td>100 Full</td>
<td>Up</td>
<td>Enable long</td>
</tr>
<tr>
<td>1/1</td>
<td>Enable</td>
<td>Down</td>
<td>N/A</td>
<td>Disable</td>
<td>N/A</td>
</tr>
<tr>
<td>1/2</td>
<td>Enable</td>
<td>Down</td>
<td>N/A</td>
<td>Disable</td>
<td>N/A</td>
</tr>
<tr>
<td>1/3</td>
<td>Enable</td>
<td>Down</td>
<td>N/A</td>
<td>Disable</td>
<td>N/A</td>
</tr>
<tr>
<td>1/4</td>
<td>Enable</td>
<td>Down</td>
<td>N/A</td>
<td>Disable</td>
<td>N/A</td>
</tr>
<tr>
<td>1/5</td>
<td>Enable</td>
<td>Down</td>
<td>N/A</td>
<td>Disable</td>
<td>N/A</td>
</tr>
<tr>
<td>1/6</td>
<td>Enable</td>
<td>Down</td>
<td>N/A</td>
<td>Disable</td>
<td>N/A</td>
</tr>
</tbody>
</table>

4.1.13 show port advertise

Use this command to display the local administrative link advertisement configuration, local operational link advertisement, and the link partner advertisement for an interface. It also displays priority Resolution for speed and duplex as per 802.3 Annex 28B.3. It displays the Auto negotiation state, Phy Master/Slave Clock configuration, and Link state of the port.

If the link is down, the Clock is displayed as No Link, and a dash is displayed against the Oper Peer advertisement, and Priority Resolution. If Auto negotiation is disabled, then the admin Local Link advertisement, operational local link advertisement, and Priority resolution fields are not displayed.

If this command is executed without the optional slot/port parameter, then it displays the Auto-negotiation state and operational Local link advertisement for all the ports. Operational link advertisement will display speed only if it is supported by both local as well as link partner. If auto-negotiation is disabled, then operational local link advertisement is not displayed.

Format  show port advertise [slot/port]

Mode  Privileged EXEC

Example: The following commands show the command output with and without the optional parameter:

(FASTPATH Switching)# show port advertise 0/1

Port: 0/1
Type: Gigabit - Level
Link State: Down
Auto Negotiation: Enabled
Clock: Auto

100f 1000h 100f 100h 10f 10h

Admin Local Link Advertisement no no yes no yes no
Oper Local Link Advertisement no no yes no yes no
Oper Peer Advertisement no no yes yes yes yes
Priority Resolution - - yes - - -

(FASTPATH Switching)# show port advertise

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Neg</th>
<th>Operational Link Advertisement</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 100h, 10f, 10h</td>
</tr>
<tr>
<td>0/2</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 100h, 10f, 10h</td>
</tr>
<tr>
<td>0/3</td>
<td>Gigabit - Level</td>
<td>Enabled</td>
<td>1000f, 100f, 100h, 10f, 10h</td>
</tr>
</tbody>
</table>
4.1.14  show port description

This command displays the interface description. Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag lag-intf-num` can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number.

**Format**    
`show port description slot/port`

**Mode**    
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>ifIndex</td>
<td>The interface index number associated with the port.</td>
</tr>
<tr>
<td>Description</td>
<td>The alpha-numeric description of the interface created by the command “description” on page 291.</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the port. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.</td>
</tr>
<tr>
<td>Bit Offset Val</td>
<td>The bit offset value.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Switching) #show port description 0/1

```
Interface............0/1
ifIndex............1
Description........
MAC address........00:10:18:82:0C:10
Bit Offset Val.....1
```

4.1.15  advertise speed

This command sets auto-negotiation advertised speed parameters to an interface or a range of interfaces. If full/half-duplex is not specified the speed is valid for both modes.

**Format**    
`advertise speed {10 | 100} [half-duplex | full-duplex]`

`advertise speed {10g | 40g} [full-duplex]`

**Mode**    
Interface Config

4.1.15.1  no advertise speed

This command resets auto-negotiation advertised speed parameters.

**Format**    
`no advertise speed {10 | 100} [half-duplex | full-duplex]`

`no advertise speed {10g | 40g} [full-duplex]`

**Mode**    
Interface Config
4.1.16 show advertise speed
This command lists the auto-negotiation advertised speed parameters. The values are listed for a specified interface.

Format  
show advertise speed unit/slot/port

Mode  
Privileged Exec

4.1.17 block
This command sets an interface or a range of interfaces in blocking mode. A blocking ports 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 ports are currently disabled, the state is not changed until they 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

4.1.17.1 no block
This command resets an interface or a range of interfaces in non-blocking mode.

Format  
no block

Mode  
Interface Config

4.1.18 show port block
This command displays the blocking mode for all or a specified port. Additionally other administrative port information (e.g. general admin mode) is displayed.

Format  
show port block {all | <slot/port>

Mode  
Privileged Exec

4.1.19 mac-learn
This command sets the HW learning for an interface. For default the HW learning mode is enabled.

Format  
mac-learn

Mode  
Interface Config

4.1.19.1 no mac-learn
If the 'no'-command is set the interface will not learn any MAC address.

Format  
no mac-learn

Mode  
Interface Config
4.1.20  show mac-learn
This command displays the HW learning mode for all or a specified port. Additionally other administrative port informa-
tion (e.g. general admin mode) is displayed.

Format  show mac-learn
Mode     Privileged Exec

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

---

**NOTICE**

STP is enabled on the switch and on all ports and LAGs by default.

---

**NOTICE**

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

---

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

Default  enabled
Format    spanning-tree
Mode      Global Config

4.2.1.1  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

4.2.2  spanning-tree auto-edge
Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount
of time.

Default  Enabled
Format    spanning-tree auto-edge
Mode      Interface Config
4.2.2.1  no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

**Format**
```
no spanning-tree auto-edge
```

**Mode**
```
Interface Config
```

4.2.3  spanning-tree backbonefast

Use this command to enable the detection of indirect link failures and accelerate spanning tree convergence on PVSTP configured switches.

Backbonefast accelerates finding an alternate path when an indirect link to the root port goes down.

Backbonefast can be configured even if the switch is configured for MST(RSTP) or PVST mode. It only has an effect when the switch is configured for the PVST mode.

If a backbonefast-enabled switch receives an inferior BPDU from its designated switch on a root or blocked port, it sets the maximum aging time on the interfaces on which it received the inferior BPDU if there are alternate paths to the designated switch. This allows a blocked port to immediately move to the listening state where the port can be transitioned to the forwarding state in the normal manner.

On receipt of an inferior BPDU from a designated bridge, backbonefast enabled switches send a Root Link Query (RLQ) request to all non-designated ports except the port from which it received the inferior BPDU. This check validates that the switch can receive packets from the root on ports where it expects to receive BPDUs. The port from which the original inferior BPDU was received is excluded because it has already encountered a failure. Designated ports are excluded as they do not lead to the root.

On receipt of an RLQ response, if the answer is negative, the receiving port has lost connection to the root and its BPDU is immediately aged out. If all nondesignated ports have already received a negative answer, the whole bridge has lost the root and can start the STP calculation from scratch.

If the answer confirms the switch can access the root bridge on a port, it can immediately age out the port on which it initially received the inferior BPDU.

A bridge that sends an RLQ puts its bridge ID in the PDU. This ensures that it does not flood the response on designated ports.

A bridge that receives an RLQ and has connectivity to the root forwards the query toward the root through its root port.

A bridge that receives a RLQ request and does not have connectivity to the root (switch bridge ID is different from the root bridge ID in the query) or is the root bridge immediately answers the query with its root bridge ID.

RLQ responses are flooded on designated ports.

**Default**
```
NA
```

**Format**
```
spanning-tree backbonefast
```

**Mode**
```
Global Config
```
4.2.3.1  no spanning-tree backbonefast
This command disables backbonefast.

**NOTICE** PVRSTP embeds support for FastBackbone and FastUplink. Even if FastUplink and FastBackbone are configured, they are effective only in PVSTP mode.

<table>
<thead>
<tr>
<th>Format</th>
<th>no spanning-tree backbonefast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.2.4  spanning-tree bpdufilter
Use this command to enable BPDU Filter on an interface or range of interfaces.

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

4.2.4.1  no spanning-tree bpdufilter
Use this command to disable BPDU Filter on the interface or range of interfaces.

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

4.2.5  spanning-tree bpdufilter default
Use this command to enable BPDU Filter on all the edge port interfaces.

| Default  | disabled                        |
| Format   | spanning-tree bpdufilter default |
| Mode     | Global Config                   |

4.2.5.1  no spanning-tree bpdufilter default
Use this command to disable BPDU Filter on all the edge port interfaces.

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

4.2.6  spanning-tree bpduflood
Use this command to enable BPDU Flood on an interface or range of interfaces.

| Default  | disabled                        |
| Format   | spanning-tree bpduflood         |
| Mode     | Interface Config               |
4.2.6.1 no spanning-tree bpduflood
Use this command to disable BPDU Flood on the interface or range of interfaces.

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

4.2.7 spanning-tree bpduguard
Use this command to enable BPDU Guard on the switch.

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

4.2.7.1 no spanning-tree bpduguard
Use this command to disable BPDU Guard on the switch.

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

4.2.8 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 RST or MST BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a no version.

Format: spanning-tree bpdumigrationcheck {slot/port | all}
Mode: Global Config

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

Default: base MAC address in hexadecimal notation
Format: spanning-tree configuration name name
Mode: Global Config
4.2.9.1 no spanning-tree configuration name
This command resets the Configuration Identifier Name to its default.

Format(no spanning-tree configuration name)
Mode Global Config

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

Default 0
Format spanning-tree configuration revision 0-65535
Mode Global Config

4.2.10.1 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

4.2.11 spanning-tree cost
Use this command to configure the external path cost for port used by a MST instance. When the auto keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a cost value from 1–200000000.

Default auto
Format spanning-tree cost {cost | auto}
Mode Interface Config

4.2.11.1 no spanning-tree cost
This command resets the auto-edge status of the port to the default value.

Format(no spanning-tree cost)
Mode Interface Config

4.2.12 spanning-tree edgeport
This command specifies that an interface (or range of interfaces) 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
4.2.12.1 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

4.2.13 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 BP DUs rather than MST BP DUs (IEEE 802.1d functionality supported).
• Use 802.1s to specify that the switch transmits MST BP DUs (IEEE 802.1s functionality supported).
• Use 802.1w to specify that the switch transmits RST BP DUs rather than MST BP DUs (IEEE 802.1w functionality supported).

4.2.13.1 no spanning-tree forceversion
This command sets the Force Protocol Version parameter to the default value.

Format: no spanning-tree forceversion
Mode: Global Config

4.2.14 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

4.2.14.1 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

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

Default: none
Format: spanning-tree guard {none | root | loop}
Mode: Interface Config
4.2.15.1 no spanning-tree guard
This command disables loop guard or root guard on the interface.

**Format**
no spanning-tree guard

**Mode**
Interface Config

4.2.16 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

4.2.16.1 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

4.2.17 spanning-tree max-hops
This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 6 to 40.

**Default**
20

**Format**
spanning-tree max-hops 6-40

**Mode**
Global Config

4.2.17.1 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
4.2.18 spanning-tree mode

This command configures global spanning tree mode per VLAN spanning tree. On a switch, only one mode can be enabled at a time.

When PVSTP or rapid PVSTP (PVRSTP) is enabled, MSTP/RSTP/STP is operationally disabled. To re-enable MSTP/RSTP/STP, disable PVSTP/PVRSTP. By default, FASTPATH has MSTP enabled. In PVSTP or PVRSTP mode, BPDUs contain per-VLAN information instead of the common spanning-tree information (MST/RSTP).

PVSTP maintains independent spanning tree information about each configured VLAN. PVSTP uses IEEE 802.1Q trunking and allows a trunked VLAN to maintain blocked or forwarding state per port on a per-VLAN basis. This allows a trunk port to be forwarded on some VLANs and blocked on other VLANs.

PVRSTP is based on the IEEE 8012.1w standard. It supports fast convergence IEEE 802.1D. PVRSTP is compatible with IEEE 802.1D spanning tree. PVRSTP sends BPDUs on all ports, instead of only the root bridge sending BPDUs, and supports the discarding, learning, and forwarding states.

When the mode is changed to PVRSTP, version 0 STP BPDUs are no longer transmitted and version 2 PVRSTP BPDUs that carry per-VLAN information are transmitted on the VLANs enabled for spanning-tree. If a version 0 BPDU is seen, PVRSTP reverts to sending version 0 BPDUs.

Per VLAN Rapid Spanning Tree Protocol (PVRSTP) embeds support for PVSTP FastBackbone and FastUplink. There is no provision to enable or disable these features in PVRSTP.

Default Disabled

Format spanning-tree mode {pvst|rapid-pvst}

Mode Global Config

4.2.18.1 no spanning-tree mode

This command globally configures the switch to the default FASTPATH spanning-tree mode, MSTP.

Format no spanning-tree mode { pvst | rapid-pvst }

Mode Global Configuration

4.2.19 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 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 in the range of 0 to 240 in increments of 16.

Default • cost—auto
• port-priority—128

Format spanning-tree mst mstid {{cost 1-200000000 | auto} | port-priority 0-240}

Mode Interface Config
4.2.19.1 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 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 | port-priority}
Mode Interface Config

4.2.20 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

4.2.20.1 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

4.2.21 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 4094.

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 4094. 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 0-4094
Mode Global Config
4.2.21 no spanning-tree mst priority
This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter \texttt{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 \texttt{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

4.2.22 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 \texttt{mstid} is a multiple spanning tree instance identifier, in the range of 0 to 4094, that corresponds to the desired existing multiple spanning tree instance. The \texttt{vlanid} can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs in the range 1 to 4093, 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 (-). Spaces and zeros are not permitted. The VLAN IDs may or may not exist in the system.

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

**Mode**
Global Config

4.2.22.1 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

4.2.23 spanning-tree port mode
This command sets the Administrative Switch Port State for this port to enabled for use by spanning tree.

**Default**
enabled

**Format**
```
spanning-tree port mode
```

**Mode**
Interface Config

4.2.23.1 no spanning-tree port mode
This command sets the Administrative Switch Port State for this port to disabled, disabling the port for use by spanning tree.

**Format**
```
no spanning-tree port mode
```

**Mode**
Interface Config

4.2.24 spanning-tree port mode all
This command sets the Administrative Switch Port State for all ports to enabled.

**Default**
enabled

**Format**
```
spanning-tree port mode all
```

**Mode**
Global Config
4.2.24.1  **no spanning-tree port mode all**
This command sets the Administrative Switch Port State for all ports to disabled.

<table>
<thead>
<tr>
<th>Format</th>
<th>no spanning-tree port mode all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.2.25  **spanning-tree port-priority**
Use this command to change the priority value of the port to allow the operator to select the relative importance of the port in the forwarding process. Set this value to a lower number to prefer a port for forwarding of frames.
All LAN ports have 128 as priority value by default. PVSTP/PVRRSTP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.
The application uses the port priority value when the LAN port is configured as an edge port.

<table>
<thead>
<tr>
<th>Default</th>
<th>enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>spanning-tree port-priority 0-248</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

4.2.26  **spanning-tree tcnguard**
Use this command to enable TCN guard on the interface. When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

<table>
<thead>
<tr>
<th>Default</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>spanning-tree tcnguard</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

4.2.26.1  **no spanning-tree tcnguard**
This command resets the TCN guard status of the port to the default value.

<table>
<thead>
<tr>
<th>Format</th>
<th>no spanning-tree tcnguard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

4.2.27  **spanning-tree transmit**
This command sets the Bridge Transmit Hold Count parameter.

<table>
<thead>
<tr>
<th>Default</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>spanning-tree transmit hold-count</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hold-count</td>
<td>The Bridge Tx hold-count parameter. The value in an integer between 1 and 10.</td>
</tr>
</tbody>
</table>
4.2.28 spanning-tree uplinkfast

Use this command to configure the rate at which gratuitous frames are sent (in packets per second) after switchover to an alternate port on PVSTP configured switches and enables uplinkfast on PVSTP switches. The range is 0-32000; the default is 150. This command has the effect of accelerating spanning-tree convergence after switchover to an alternate port.

Uplinkfast can be configured even if the switch is configured for MST(RSTP) mode, but it only has an effect when the switch is configured for PVST mode. Enabling FastUplink increases the priority by 3000. Path costs less than 3000 have an additional 3000 added when uplinkfast is enabled. This reduces the probability that the switch will become the root switch.

Uplinkfast immediately changes to an alternate root port on detecting a root port failure and changes the new root port directly to the forwarding state. A TCN is sent for this event.

After a switchover to an alternate port (new root port), uplinkfast multicasts a gratuitous frame on the new root port on behalf of each attached machine so that the rest of the network knows to use the secondary link to reach that machine.

PVRSTP embeds support for backbonefast and uplinkfast. There is no provision to enable or disable these features in PVRSTP configured switches.

Default

Format

Mode

Global Config

4.2.28.1 no spanning-tree uplinkfast

This command disables uplinkfast on PVSTP configured switches. All switch priorities and path costs that have not been modified from their default values are set to their default values.

Default

Format

Mode

Global Config

4.2.29 spanning-tree vlan

Use this command to enable/disable spanning tree on a VLAN.

Default

Format

Mode

Global Config

4.2.30 spanning-tree vlan cost

Use this command to set the path cost for a port in a VLAN. The valid values are in the range of 1 to 200000000 or auto. If auto is selected, the path cost value is set based on the link speed.

Default

Format

Mode

Interface Config
4.2.31 spanning-tree vlan forward-time

Use this command to configure the spanning tree forward delay time for a VLAN or a set of VLANs. The default is 15 seconds.

Set this value to a lower number to accelerate the transition to forwarding. The network operator should take into account the end-to-end BPDU propagation delay, the maximum frame lifetime, the maximum transmission halt delay, and the message age overestimate values specific to their network when configuring this parameter.

**Default** 15 seconds

**Format** spanning-tree vlan vlan-list forward-time 4-30

**Mode** Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLANs to which to apply this command.</td>
</tr>
<tr>
<td>forward-time</td>
<td>The spanning tree forward delay time. The range is 4-30 seconds.</td>
</tr>
</tbody>
</table>

4.2.32 spanning-tree vlan hello-time

Use this command to configure the spanning tree hello time for a specified VLAN or a range of VLANs. The default is 2 seconds. Set this value to a lower number to accelerate the discovery of topology changes.

**Default** 2 seconds

**Format** spanning-tree vlan vlan-list hello-time 1-10

**Mode** Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLANs to which to apply this command.</td>
</tr>
<tr>
<td>hello-time</td>
<td>The spanning tree forward hello time. The range is 1-10 seconds.</td>
</tr>
</tbody>
</table>

4.2.33 spanning-tree vlan max-age

Use this command to configure the spanning tree maximum age time for a set of VLANs. The default is 20 seconds.

Set this value to a lower number to accelerate the discovery of topology changes. The network operator must take into account the end-to-end BPDU propagation delay and message age overestimate for their specific topology when configuring this value.

The default setting of 20 seconds is suitable for a network of diameter 7, lost message value of 3, transit delay of 1, hello interval of 2 seconds, overestimate per bridge of 1 second, and a BPDU delay of 1 second. For a network of diameter 4, a setting of 16 seconds is appropriate if all other timers remain at their default values.

**Default** 20 seconds

**Format** spanning-tree vlan vlan-list max-age 6-40

**Mode** Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLANs to which to apply this command.</td>
</tr>
<tr>
<td>hello-time</td>
<td>The spanning tree forward hello time. The range is 1-10 seconds.</td>
</tr>
</tbody>
</table>
4.2.34 spanning-tree vlan root

Use this command to configure the switch to become the root bridge or standby root bridge by modifying the bridge priority from the default value of 32768 to a lower value calculated to ensure the bridge is the root (or standby) bridge. The logic takes care of setting the bridge priority to a value lower (primary) or next lower (secondary) than the lowest bridge priority for the specified VLAN or a range of VLANs.

Default 32768
Format spanning-tree vlan vlan-list root {primary|secondary}
Mode Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLANs to which to apply this command.</td>
</tr>
</tbody>
</table>

4.2.35 spanning-tree vlan port-priority

Use this command to change the VLAN port priority value of the VLAN port to allow the operator to select the relative importance of the VLAN port in the forwarding selection process when the port is configured as a point-to-point link type. Set this value to a lower number to prefer a port for forwarding of frames.

Default None
Format spanning-tree vlan vlan-id port-priority priority
Mode Interface Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLANs to which to apply this command.</td>
</tr>
<tr>
<td>priority</td>
<td>The VLAN port priority. The range is 0-255.</td>
</tr>
</tbody>
</table>

4.2.36 spanning-tree vlan priority

Use this command to configure the bridge priority of a VLAN. The default value is 32768. If the value configured is not among the specified values, it will be rounded off to the nearest valid value.

Default 32768
Format spanning-tree vlan vlan-list priority priority
Mode Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLANs to which to apply this command.</td>
</tr>
<tr>
<td>priority</td>
<td>The VLAN bridge priority. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.</td>
</tr>
</tbody>
</table>
4.2.37  show spanning-tree

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

**Format**  
show spanning-tree

**Mode**  
- Privileged EXEC
- User EXEC

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

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

(FASTPATH Routing) #show spanning-tree

Bridge Priority.......................... 32768
Bridge Identifier........................ 80:00:00:10:18:48:FC:07
Time Since Topology Change............. 8 day 3 hr 22 min 37 sec
Topology Change Count................... 0
Topology Change in progress............. FALSE
Designated Root.......................... 80:00:00:10:18:48:FC:07
Root Path Cost......................... 0
Root Port Identifier.................... 00:00
Bridge Max Age......................... 20
Bridge Max Hops......................... 20
Bridge Tx Hold Count................... 6
Bridge Forwarding Delay............... 15
Hello Time................................ 2
Bridge Hold Time......................... 6
4.2.38  show spanning-tree backbonefast

This command displays spanning tree information for backbonefast.

**Format**  
show spanning-tree backbonefast

**Mode**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transitions via Backbonefast</td>
<td>The number of backbonefast transitions.</td>
</tr>
<tr>
<td>Inferior BPDU received (all VLANs)</td>
<td>The number of inferior BPDU received on all VLANs.</td>
</tr>
<tr>
<td>RLQ request PDUs received (all VLANs)</td>
<td>The number of root link query (RLQ) requests PDUs received on all VLANs.</td>
</tr>
<tr>
<td>RLQ response PDUs received (all VLANs)</td>
<td>The number of RLQ response PDUs received on all VLANs.</td>
</tr>
<tr>
<td>RLQ request PDUs sent (all VLANs)</td>
<td>The number of RLQ request PDUs sent on all VLANs.</td>
</tr>
<tr>
<td>RLQ response PDUs sent (all VLANs)</td>
<td>The number of RLQ response PDUs sent on all VLANs.</td>
</tr>
</tbody>
</table>

**Example:** The following shows example output from the command.

```
(Routing)#show spanning-tree backbonefast
```

Backbonefast Statistics

<table>
<thead>
<tr>
<th>Term</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transitions via Backbonefast</td>
<td>0</td>
</tr>
<tr>
<td>Inferior BPDU received (all VLANs)</td>
<td>0</td>
</tr>
<tr>
<td>RLQ request PDUs received (all VLANs)</td>
<td>0</td>
</tr>
<tr>
<td>RLQ response PDUs received (all VLANs)</td>
<td>0</td>
</tr>
<tr>
<td>RLQ request PDUs sent (all VLANs)</td>
<td>0</td>
</tr>
<tr>
<td>RLQ response PDUs sent (all VLANs)</td>
<td>0</td>
</tr>
</tbody>
</table>

4.2.39  show spanning-tree brief

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

**Format**  
show spanning-tree brief

**Mode**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Priority</td>
<td>Configured value.</td>
</tr>
<tr>
<td>Bridge Identifier</td>
<td>The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Bridge Max Age</td>
<td>Configured value.</td>
</tr>
<tr>
<td>Bridge Max Hops</td>
<td>Bridge max-hops count for the device.</td>
</tr>
<tr>
<td>Bridge Hello Time</td>
<td>Configured value.</td>
</tr>
<tr>
<td>Bridge Forward Delay</td>
<td>Configured value.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(FASTPATH Routing) #show spanning-tree brief

```
Bridge Priority.......................... 32768
Bridge Identifier........................ 80:00:00:10:18:48:FC:07
Bridge Max Age.......................... 20
Bridge Max Hops.......................... 20
Bridge Hello Time........................ 2
Bridge Forward Delay...................... 15
Bridge Hold Time.......................... 6
```

(FASTPATH Routing) #

### 4.2.40 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. Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag lag-intf-num` can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number. The following details are displayed on execution of the command.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Time</td>
<td>Admin hello time for this port.</td>
</tr>
<tr>
<td>Port Mode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>BPDU Guard Effect</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>Root Guard</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>Loop Guard</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>TCN Guard</td>
<td>Enable or disable the propagation of received topology change notifications and topology changes to other ports.</td>
</tr>
<tr>
<td>BPDU Filter Mode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>BPDU Flood Mode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>Auto Edge</td>
<td>To enable or disable the feature that causes a port that has not seen a BPDU for edge delay time, to become an edge port and transition to forwarding faster.</td>
</tr>
<tr>
<td>Port Up Time Since Counters Last Cleared</td>
<td>Time since port was reset, displayed in days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>STP BDUs Transmitted</td>
<td>Spanning Tree Protocol Bridge Protocol Data Units sent.</td>
</tr>
<tr>
<td>STP BDUs Received</td>
<td>Spanning Tree Protocol Bridge Protocol Data Units received.</td>
</tr>
<tr>
<td>RSTP BDUs Transmitted</td>
<td>Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.</td>
</tr>
<tr>
<td>RSTP BDUs Received</td>
<td>Rapid Spanning Tree Protocol Bridge Protocol Data Units received.</td>
</tr>
<tr>
<td>MSTP BDUs Transmitted</td>
<td>Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.</td>
</tr>
<tr>
<td>MSTP BDUs Received</td>
<td>Multiple Spanning Tree Protocol Bridge Protocol Data Units received.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(FASTPATH Routing) > show spanning-tree interface 0/1

Hello Time................................. Not Configured
Port Mode................................. Enabled
BPDU Guard Effect....................... Disabled
Root Guard................................ FALSE
Loop Guard................................ FALSE
TCN Guard................................ FALSE
BPDU Filter Mode......................... Disabled
BPDU Flood Mode........................ Disabled
Auto Edge.................................... TRUE
Port Up Time Since Counters Last Cleared...... 8 day 3 hr 39 min 58 sec
STP BPDUs Transmitted.................... 0
STP BPDUs Received....................... 0
RSTP BPDUs Transmitted................. 0
RSTP BPDUs Received..................... 0
MSTP BPDUs Transmitted............... 0
MSTP BPDUs Received.................... 0

(FASTPATH Routing) >

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

(FASTPATH Routing) > show spanning-tree interface lag 1

Hello Time................................. Not Configured
Port Mode................................. Enabled
BPDU Guard Effect....................... Disabled
Root Guard................................ FALSE
Loop Guard................................ FALSE
TCN Guard................................ FALSE
BPDU Filter Mode......................... Disabled
BPDU Flood Mode........................ Disabled
Auto Edge.................................... TRUE
Port Up Time Since Counters Last Cleared...... 8 day 3 hr 42 min 5 sec
STP BPDUs Transmitted.................... 0
STP BPDUs Received....................... 0
RSTP BPDUs Transmitted................. 0
RSTP BPDUs Received..................... 0
MSTP BPDUs Transmitted............... 0
MSTP BPDUs Received.................... 0

(FASTPATH Routing) >

4.2.41 show spanning-tree mst detailed

This command displays the detailed settings for an MST instance.

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree mst detailed mstid</td>
<td>A multiple spanning tree instance identifier. The value is 0–4094.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(FASTPATH Routing) \> show spanning-tree mst detailed 0

MST Instance ID................................. 0
MST Bridge Priority............................ 32768
MST Bridge Identifier......................... 80:00:00:10:18:48:FC:07
Time Since Topology Change.................. 8 day 3 hr 47 min 7 sec
Topology Change Count........................ 0
Topology Change in progress.................. FALSE
Designated Root.................................. 80:00:00:10:18:48:FC:07
Root Path Cost.................................. 0
Root Port Identifier......................... 00:00

Associated FIDs | Associated VLANs
-----------------|-------------------

(FASTPATH Routing) \>

### 4.2.42 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. Instead of **slot/port**, **lag lag-intf-num** can be used as an alternate way to specify the LAG interface. **lag lag-intf-num** can also be used to specify the LAG interface where **lag-intf-num** is the LAG port number.

**Format**

```
show spanning-tree mst port detailed mstid slot/port|lag lag-intf-num
```

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST Instance ID</td>
<td>The ID of the existing multiple spanning tree (MST) instance identifier. The value is 0–4094.</td>
</tr>
<tr>
<td>Port Identifier</td>
<td>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.</td>
</tr>
<tr>
<td>Port Priority</td>
<td>The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.</td>
</tr>
<tr>
<td>Port Forwarding State</td>
<td>Current spanning tree state of this port.</td>
</tr>
<tr>
<td>Port Role</td>
<td>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</td>
</tr>
<tr>
<td>Auto-Calculate Port Path Cost</td>
<td>Indicates whether auto calculation for port path cost is enabled.</td>
</tr>
<tr>
<td>Port Path Cost</td>
<td>Configured value of the Internal Port Path Cost parameter.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The Identifier of the designated root for this port.</td>
</tr>
<tr>
<td>Root Path Cost</td>
<td>The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.</td>
</tr>
<tr>
<td>Designated Bridge</td>
<td>Bridge Identifier of the bridge with the Designated Port.</td>
</tr>
<tr>
<td>Designated Port Identifier</td>
<td>Port on the Designated Bridge that offers the lowest cost to the LAN.</td>
</tr>
<tr>
<td>Loop Inconsistent State</td>
<td>The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.</td>
</tr>
<tr>
<td>Transitions Into Loop Inconsistent State</td>
<td>The number of times this interface has transitioned into loop inconsistent state.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transitions Out of Loop Inconsistent State</td>
<td>The number of times this interface has transitioned out of loop inconsistent state.</td>
</tr>
<tr>
<td>Port Identifier</td>
<td>The port identifier for this port within the CST.</td>
</tr>
<tr>
<td>Port Priority</td>
<td>The priority of the port within the CST.</td>
</tr>
<tr>
<td>Port Forwarding State</td>
<td>The forwarding state of the port within the CST.</td>
</tr>
<tr>
<td>Port Role</td>
<td>The role of the specified interface within the CST.</td>
</tr>
<tr>
<td>Auto-Calculate Port Path Cost</td>
<td>Indicates whether auto calculation for port path cost is enabled or not (disabled).</td>
</tr>
<tr>
<td>Port Path Cost</td>
<td>The configured path cost for the specified interface.</td>
</tr>
<tr>
<td>Auto-Calculate External Port Path Cost</td>
<td>Indicates whether auto calculation for external port path cost is enabled.</td>
</tr>
<tr>
<td>External Port Path Cost</td>
<td>The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.</td>
</tr>
<tr>
<td>Designated Root Identifier</td>
<td>Identifier of the designated root for this port within the CST.</td>
</tr>
<tr>
<td>Root Path Cost</td>
<td>The root path cost to the LAN by the port.</td>
</tr>
<tr>
<td>Designated Bridge</td>
<td>The bridge containing the designated port.</td>
</tr>
<tr>
<td>Designated Port Identifier</td>
<td>Port on the Designated Bridge that offers the lowest cost to the LAN.</td>
</tr>
<tr>
<td>Topology Change Acknowledgement</td>
<td>Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>The hello time in use for this port.</td>
</tr>
<tr>
<td>Edge Port</td>
<td>The configured value indicating if this port is an edge port.</td>
</tr>
<tr>
<td>Edge Port Status</td>
<td>The derived value of the edge port status. True if operating as an edge port; false otherwise.</td>
</tr>
<tr>
<td>Point To Point MAC Status</td>
<td>Derived value indicating if this port is part of a point to point link.</td>
</tr>
<tr>
<td>CST Regional Root</td>
<td>The regional root identifier in use for this port.</td>
</tr>
<tr>
<td>CST Internal Root Path Cost</td>
<td>The internal root path cost to the LAN by the designated external port.</td>
</tr>
<tr>
<td>Loop Inconsistent State</td>
<td>The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.</td>
</tr>
<tr>
<td>Transitions Into Loop Inconsistent State</td>
<td>The number of times this interface has transitioned into loop inconsistent state.</td>
</tr>
<tr>
<td>Transitions Out of Loop Inconsistent State</td>
<td>The number of times this interface has transitioned out of loop inconsistent state.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command in slot/port format.

```plaintext
(FASTPATH Routing) > show spanning-tree mst port detailed 0 0/1
```

- **Port Identifier**: 80:01
- **Port Priority**: 128
- **Port Forwarding State**: Disabled
- **Port Role**: Disabled
- **Auto-calculate Port Path Cost**: Enabled
- **Port Path Cost**: 0
- **Auto-Calculate External Port Path Cost**: Enabled
- **External Port Path Cost**: 0
- **Designated Root**: 80:00:00:10:18:48:FC:07
- **Root Path Cost**: 0
- **Designated Bridge**: 80:00:00:10:18:48:FC:07
- **Designated Port Identifier**: 00:00
- **Topology Change Acknowledge**: FALSE
- **Hello Time**: 2
- **Edge Port**: FALSE
- **Edge Port Status**: FALSE
- **Point to Point MAC Status**: TRUE
- **CST Regional Root**: 80:00:00:10:18:48:FC:07
- **CST Internal Root Path Cost**: 0
- **Loop Inconsistent State**: FALSE
- **Transitions Into Loop Inconsistent State**: 0
- **Transitions Out Of Loop Inconsistent State**: 0

**Example:** The following shows example CLI display output for the command using a LAG interface number.

```plaintext
(FASTPATH Routing) > show spanning-tree mst port detailed 0 lag 1
```

- **Port Identifier**: 60:42
- **Port Priority**: 96
- **Port Forwarding State**: Disabled
- **Port Role**: Disabled
- **Auto-calculate Port Path Cost**: Enabled
- **Port Path Cost**: 0
- **Auto-Calculate External Port Path Cost**: Enabled
- **External Port Path Cost**: 0
- **Designated Root**: 80:00:00:10:18:48:FC:07
- **Root Path Cost**: 0
- **Designated Bridge**: 80:00:00:10:18:48:FC:07
- **Designated Port Identifier**: 00:00
- **Topology Change Acknowledge**: FALSE
- **Hello Time**: 2
- **Edge Port**: FALSE
- **Edge Port Status**: FALSE
- **Point to Point MAC Status**: TRUE
- **CST Regional Root**: 80:00:00:10:18:48:FC:07
- **CST Internal Root Path Cost**: 0
- **Loop Inconsistent State**: FALSE
- **Transitions Into Loop Inconsistent State**: 0
- **Transitions Out Of Loop Inconsistent State**: 0

---

**Example:** The following shows example CLI display output for the command using a LAG interface number.

```plaintext
(FASTPATH Routing) >
```
4.2.43 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 \texttt{mstid} indicates a particular MST instance. The parameter \texttt{(slot/port|all)} indicates the desired switch port or all ports. Instead of \texttt{slot/port}, \texttt{lag lag-intf-num} can be used as an alternate way to specify the LAG interface. \texttt{lag lag-intf-num} can also be used to specify the LAG interface where \texttt{lag-intf-num} is the LAG port number.

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

\textbf{Format:} \texttt{show spanning-tree mst port summary mstid \{slot/port | lag lag-intf-num | all\}}

\textbf{Mode:}
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST Instance ID</td>
<td>The MST instance associated with this port.</td>
</tr>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>STP Mode</td>
<td>Indicates whether spanning tree is enabled or disabled on the port.</td>
</tr>
<tr>
<td>Type</td>
<td>Currently not used.</td>
</tr>
<tr>
<td>STP State</td>
<td>The forwarding state of the port in the specified spanning tree instance.</td>
</tr>
<tr>
<td>Port Role</td>
<td>The role of the specified port within the spanning tree.</td>
</tr>
<tr>
<td>Desc</td>
<td>Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.</td>
</tr>
</tbody>
</table>

\textbf{Example:} The following shows example CLI display output for the command in \texttt{slot/port} format.

(FASTPATH Routing) \texttt{>show spanning-tree mst port summary 0 0/1}

\begin{verbatim}
MST Instance ID................................. CST

<table>
<thead>
<tr>
<th>Interface</th>
<th>STP Mode</th>
<th>Type</th>
<th>STP State</th>
<th>Port Role</th>
<th>Desc</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>
\end{verbatim}

\textbf{Example:} The following shows example CLI display output for the command using a LAG interface number.

(FASTPATH Routing) \texttt{>show spanning-tree mst port summary 0 lag 1}

\begin{verbatim}
MST Instance ID................................. CST

<table>
<thead>
<tr>
<th>Interface</th>
<th>STP Mode</th>
<th>Type</th>
<th>STP State</th>
<th>Port Role</th>
<th>Desc</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/1</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>
\end{verbatim}

4.2.44 show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

\textbf{Format:} \texttt{show spanning-tree mst port summary mstid active}

\textbf{Mode:}
- Privileged EXEC
- User EXEC
Example: The following shows example CLI display output for the command.

```
(FASTPATH Routing) > show spanning-tree mst port summary 0 active
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>STP Mode</th>
<th>Type</th>
<th>STP State</th>
<th>Port Role</th>
<th>Desc</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.2.45 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

### 4.2.46 show spanning-tree summary

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

**Format**

```
show spanning-tree summary
```

**Mode**

- Privileged EXEC
- User EXEC

---

**Term** | **Definition**
--- | ---
MST Instance ID | The ID of the existing MST instance.

**Term** | **Definition**
--- | ---
STP Mode | Indicates whether spanning tree is enabled or disabled on the port.

**Term** | **Definition**
--- | ---
Type | Currently not used.

**Term** | **Definition**
--- | ---
STP State | The forwarding state of the port in the specified spanning tree instance.

**Term** | **Definition**
--- | ---
Port Role | The role of the specified port within the spanning tree.

**Term** | **Definition**
--- | ---
Desc | Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

**Term** | **Definition**
--- | ---
MST Instance ID List | List of multiple spanning trees IDs currently configured.

**Term** | **Definition**
--- | ---
For each MSTID: |  
  - Associated FIDs | List of forwarding database identifiers associated with this instance.
  - Associated VLANs | List of VLAN IDs associated with this instance.

**Term** | **Definition**
--- | ---
Spanning Tree Adminmode | Enabled or disabled.

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

**Term** | **Definition**
--- | ---
BPDU Guard Mode | Enabled or disabled.

**Term** | **Definition**
--- | ---
BPDU Filter Mode | Enabled or disabled.
Example: The following shows example CLI display output for the command.

(FASTPATH Routing) >show spanning-tree summary

Spanning Tree Adminmode........... Enabled
Spanning Tree Version............. IEEE 802.1s
BPDU Guard Mode.................. Disabled
BPDU Filter Mode.................. Disabled
Configuration Name................ ****
Configuration Revision Level....... ****
Configuration Digest Key........... ****
Configuration Format Selector..... 0
No MST instances to display.

4.2.47 show spanning-tree uplinkfast

This command displays spanning tree information for uplinkfast.

Format show spanning-tree uplinkfast
Mode
  • Privileged EXEC
  • User EXEC

Example: The following shows example output from the command.

(Routing) #show spanning-tree uplinkfast

Uplinkfast is enabled.
BPDU update rate : 150 packets/sec

Uplinkfast Statistics
-----------------------
Uplinkfast transitions (all VLANs)............. 0
Proxy multicast addresses transmitted (all VLANs)... 0

4.2.48 show spanning-tree vlan

This command displays spanning tree information per VLAN and also lists out the port roles and states along with port cost. The vlan-list parameter is a list of VLANs or VLAN-ranges separated by commas and with no embedded blank spaces. VLAN ranges are of the form "X-Y" where X and Y are valid VLAN identifiers and X< Y. The vlanid corresponds to an existing VLAN ID.

Format show spanning-tree vlan {vlanid | vlan-list}
Mode
  • Privileged EXEC
  • User EXEC
**Example:** The following shows example CLI display output for the command.

```
(Routing) show spanning-tree vlan 1
```

**VLAN 1**

```plaintext
Spanning-tree enabled protocol rpvst
RootID  Priority  32769
Address  00:0C:29:03:80:EA
Cost  0
Port  This switch is the root

Hello Time  2 Sec Max Age  15 sec Forward Delay  15 sec
BridgeID  Priority  32769 (priority 32768 sys-id-ext 1)
Address  00:0C:29:03:80:EA
Hello Time  2 Sec Max Age  15 sec Forward Delay  15 sec
Aging Time  300
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Designated</td>
<td>Forwarding</td>
<td>3000</td>
<td>128.1</td>
</tr>
<tr>
<td>0/2</td>
<td>Designated</td>
<td>Forwarding</td>
<td>3000</td>
<td>128.2</td>
</tr>
<tr>
<td>0/3</td>
<td>Disabled</td>
<td>Disabled</td>
<td>3000</td>
<td>128.3</td>
</tr>
<tr>
<td>0/4</td>
<td>Designated</td>
<td>Forwarding</td>
<td>3000</td>
<td>128.4</td>
</tr>
<tr>
<td>0/5</td>
<td>Designated</td>
<td>Forwarding</td>
<td>3000</td>
<td>128.5</td>
</tr>
<tr>
<td>0/6</td>
<td>Designated</td>
<td>Forwarding</td>
<td>3000</td>
<td>128.6</td>
</tr>
<tr>
<td>0/7</td>
<td>Designated</td>
<td>Forwarding</td>
<td>3000</td>
<td>128.7</td>
</tr>
<tr>
<td>0/8</td>
<td>Designated</td>
<td>Forwarding</td>
<td>3000</td>
<td>128.8</td>
</tr>
<tr>
<td>1/1</td>
<td>Disabled</td>
<td>Disabled</td>
<td>3000</td>
<td>128.1026</td>
</tr>
<tr>
<td>1/2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>3000</td>
<td>128.1027</td>
</tr>
<tr>
<td>1/3</td>
<td>Disabled</td>
<td>Disabled</td>
<td>3000</td>
<td>128.1028</td>
</tr>
<tr>
<td>1/4</td>
<td>Disabled</td>
<td>Disabled</td>
<td>3000</td>
<td>128.1029</td>
</tr>
<tr>
<td>1/5</td>
<td>Disabled</td>
<td>Disabled</td>
<td>3000</td>
<td>128.1030</td>
</tr>
<tr>
<td>1/6</td>
<td>Disabled</td>
<td>Disabled</td>
<td>3000</td>
<td>128.1031</td>
</tr>
</tbody>
</table>

### 4.3 Loop Protection Commands

This section describes the commands used to configure loop protection. Loop protection detects physical and logical loops between Ethernet ports on a device. Loop protection must be enabled globally before it can be enabled at the interface level.

#### 4.3.1 keepalive (Global Config)

This command enables loop protection for the system.

**Default**  Disabled  
**Format**  keepalive  
**Mode**  Global Config
4.3.1  no keepalive
This command disables loop protection for the system. This command also sets the transmit interval and retry count to the default value.

Format  no keepalive
Mode    Global Config

4.3.2  keepalive (Interface Config)
This command enables keepalive on a particular interface.

Default None
Format keepalive
Mode    Interface Config

4.3.2.1  no keepalive
This command disables keepalive on a particular interface.

Format keepalive
Mode    Interface Config

4.3.3  keepalive action
This command configures the action to be taken on a port when a loop is detected.

Default Disabled.
Format keepalive receive-action {log|disable|both}
Mode    Interface Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Only logs the message. The log mode only logs the message to buffer logs without bringing the port down.</td>
</tr>
<tr>
<td>disable</td>
<td>Shuts down the port. This is the default.</td>
</tr>
<tr>
<td>both</td>
<td>Logs and disables the port.</td>
</tr>
</tbody>
</table>

4.3.3.1  no keepalive action
This command returns the command to the default action of disabling a port when a loop is detected.

Format no keepalive receive-action {log|disable|both}
Mode    Interface Configuration

4.3.4  keepalive disable-timer
This command configures the time, in seconds, for which a port is down if a loop is detected. The default time is 0 so that port needs to be re-enabled manually to bring it up.

Default 0
Format keep-alive disable-timer value
Mode    Global Configuration
4.3.4.1  no keepalive disable-timer
This command removes the disable-timer.

**Format**  
`no keep-alive disable-timer`

**Mode**  
Global Configuration

4.3.5  keepalive retry
This command configures the time in seconds between transmission of keep-alive packets. Retry is an optional parameter that configures the count of keepalive packets received by the switch after which the interface will be error disabled.

**Default**  
5

**Format**  
`keepalive val [retry]`

**Mode**  
Global Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>val</td>
<td>The time in seconds between transmission of keep-alive packets.</td>
</tr>
<tr>
<td>retry</td>
<td>Configures the count of keepalive packets received by the switch after which the switch will be error disabled.</td>
</tr>
</tbody>
</table>

4.3.6  show keepalive
This command displays the global keepalive configuration.

**Default**  
None

**Format**  
`show keepalive`

**Mode**  
Privileged EXEC

**Example:**
(Routing) #show keepalive
Keepalive     : Enabled
Transmit interval : 5 seconds
Retry count     : 1

4.3.7  show keepalive statistics
This command displays the keepalive statistics for each port or a specific port.

**Default**  
None

**Format**  
`show keepalive statistics {port-num | all}`

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-num</td>
<td>The port number for which to show statistics.</td>
</tr>
</tbody>
</table>
### Example:

(Routing) `#show keepalive statistics all`

<table>
<thead>
<tr>
<th>Port</th>
<th>Keep Alive</th>
<th>Loop Detected</th>
<th>Loop Count</th>
<th>Time Since Last Loop</th>
<th>Rx Port Alive</th>
<th>Rx Port Detected</th>
<th>Rx Port Count</th>
<th>Rx Port Time Since Last Loop</th>
<th>Rx Port Action</th>
<th>Rx Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>85</td>
<td>shut-down</td>
<td>D-Disable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/3</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
<td>log-shutdown</td>
<td>Enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 4.3.8 clear counters keepalive

This command clears keepalive statistics associated with ports (for example, number of transmitted packets, received packets, and loop packets).

**Default** None

**Format** `clear counters keepalive`

**Mode** Privileged EXEC

### 4.4 VLAN Commands

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

#### 4.4.1 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

#### 4.4.2 network mgmt_vlan

This command configures the Management VLAN ID.

**Default** 1

**Format** `network mgmt_vlan 1-4093`

**Mode** Privileged EXEC

#### 4.4.2.1 no network mgmt_vlan

This command sets the Management VLAN ID to the default.

**Format** `no network mgmt_vlan`

**Mode** Privileged EXEC

#### 4.4.3 vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-4093.

**Format** `vlan 2-4093`

**Mode** VLAN Config
4.4.3.1 no vlan
This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 2-4093.

Format
no vlan 2-4093
Mode
VLAN Config

4.4.4 vlan acceptframe
This command sets the frame acceptance mode on an interface or range of interfaces. 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. For admituntaggedonly mode, only untagged frames are accepted on this interface; tagged frames are discarded. With any option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

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

4.4.4.1 no vlan acceptframe
This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format
no vlan acceptframe
Mode
Interface Config

4.4.5 vlan ingressfilter
This command enables ingress filtering on an interface or range of interfaces. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default
disabled
Format
vlan ingressfilter
Mode
Interface Config

4.4.5.1 no vlan ingressfilter
This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format
no vlan ingressfilter
Mode
Interface Config
4.4.6 vlan internal allocation

Use this command to configure which VLAN IDs to use for port-based routing interfaces. When a port-based routing interface is created, an unused VLAN ID is assigned internally.

**Format**  
`vlan internal allocation {base vlan-id | policy ascending | policy descending}`

**Mode**  
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>base vlan-id</code></td>
<td>The first VLAN ID to be assigned to a port-based routing interface.</td>
</tr>
<tr>
<td><code>policy ascending</code></td>
<td>VLAN IDs assigned to port-based routing interfaces start at the base and increase in value.</td>
</tr>
<tr>
<td><code>policy descending</code></td>
<td>VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value.</td>
</tr>
</tbody>
</table>

4.4.7 vlan makestatic

This command changes a dynamically created VLAN (created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

**Format**  
`vlan makestatic 2-4093`

**Mode**  
VLAN Config

4.4.8 vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4093.

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

**Format**  
`vlan name 1-4093 name`

**Mode**  
VLAN Config

4.4.8.1 no vlan name

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

**Format**  
`no vlan name 1-4093`

**Mode**  
VLAN Config

4.4.9 vlan participation

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

**Format**  
`vlan participation {exclude | include | auto} 1-4093`

**Mode**  
Interface Config

Participation options are:
4.4.10  vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

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

**Mode**  
Global Config

You can use the following participation options:

<table>
<thead>
<tr>
<th>Options</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>include</td>
<td>The interface is always a member of this VLAN. This is equivalent to registration fixed.</td>
</tr>
<tr>
<td>exclude</td>
<td>The interface is never a member of this VLAN. This is equivalent to registration forbidden.</td>
</tr>
<tr>
<td>auto</td>
<td>The interface is dynamically registered in this VLAN by GVRP and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.</td>
</tr>
</tbody>
</table>

4.4.11  vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

**Default**  
all

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

**Mode**  
Global Config

The modes are defined as follows:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Only mode</td>
<td>Untagged frames or priority frames received on this interface are discarded.</td>
</tr>
<tr>
<td>Admit Untagged Only mode</td>
<td>VLAN-tagged and priority tagged frames received on this interface are discarded.</td>
</tr>
<tr>
<td>Admit All mode</td>
<td>Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.</td>
</tr>
</tbody>
</table>

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.
4.4.11  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

4.4.12  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

4.4.12.1  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

4.4.13  vlan port pvid all
This command changes the VLAN ID for all interface.

Default  1
Format  vlan port pvid all 1-4093
Mode    Global Config

4.4.13.1  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

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

Format  vlan port tagging all 1-4093
Mode    Global Config
4.4.14.1  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

4.4.15  vlan protocol group
This command adds protocol-based VLAN groups to the system. The groupid is a unique number from 1–128 that is used
to identify the group in subsequent commands.

Format    vlan protocol group groupid
Mode       Global Config

4.4.16  vlan protocol group name
This command assigns a name to a protocol-based VLAN groups. The groupname variable can be a character string of 0
to 16 characters.

Format    vlan protocol group name groupid groupname
Mode       Global Config

4.4.16.1  no vlan protocol group name
This command removes the name from the group identified by groupid.

Format    no vlan protocol group name groupid
Mode       Global Config

4.4.17  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 and hexadecimal or decimal values ranging from 0x0600 (1536) to 0xFFFF (65535). The protocol list can accept up to 16 protocols separated by a comma.

Default    none
Format    vlan protocol group add protocol groupid ethertype protocol-list
Mode       Global Config
4.4.17.1   no vlan protocol group add protocol
This command removes the protocols specified in the protocol-list from this protocol-based VLAN group that is identified by this groupid.

Format          no vlan protocol group add protocol groupid ethertype protocol-list
Mode            Global Config

4.4.18   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

4.4.18.1   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

4.4.19   protocol vlan group
This command adds a physical interface or a range of 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 fails and the interface(s) are not added to the group.

Default          none
Format           protocol vlan group groupid
Mode             Interface Config

4.4.19.1   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

4.4.20   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
4.4.20.1  **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

4.4.21  **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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The group name of an entry in the Protocol-based VLAN table.</td>
</tr>
<tr>
<td>Group ID</td>
<td>The group identifier of the protocol group.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN associated with this Protocol Group.</td>
</tr>
<tr>
<td>Protocol(s)</td>
<td>The type of protocol(s) for this group.</td>
</tr>
<tr>
<td>Interface(s)</td>
<td>Lists the <em>slot/port</em> interface(s) that are associated with this Protocol Group.</td>
</tr>
</tbody>
</table>

4.4.22  **vlan pvid**
This command changes the VLAN ID on an interface or range of interfaces.

**Default**

1

**Format**

```
vlan pvid 1-4093
```

**Mode**

Interface Config

4.4.22.1  **no vlan pvid**
This command sets the VLAN ID on an interface or range of interfaces to 1.

**Format**

```
no vlan pvid
```

**Mode**

Interface Config

4.4.23  **vlan tagging**
This command configures the tagging behavior for a specific interface or range of 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 tagging 1-4093
```

**Mode**

- Interface Config
4.4.23.1 no vlan tagging
This command configures the tagging behavior for a specific interface or range of 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 tagging 1-4093
Mode
• Interface Config

4.4.24 vlan association subnet
This command associates a VLAN to a specific IP-subnet.

Format
vlan association subnet ipaddr netmask vlanid
Mode
VLAN Config

4.4.24.1 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

4.4.25 vlan association mac
This command associates a MAC address to a VLAN.

Format
vlan association mac macaddr vlanid
Mode
VLAN database

4.4.25.1 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

4.4.26 remote-span
This command identifies the VLAN as the RSPAN VLAN.

Default
None
Format
remote-span
Mode
VLAN configuration

4.4.27 show vlan
This command displays information about the configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and the ports which belong to a private VLAN.

Format
show vlan {vlanid|private-vlan [type]}
Mode
• Privileged EXEC
• User EXEC
### 4.4.28 `show vlan internal usage`

This command displays information about the VLAN ID allocation on the switch.

**Format**  
`show vlan internal usage`

**Mode**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary</strong></td>
<td>Primary VLAN identifier. The range of the VLAN ID is 1 to 4093.</td>
</tr>
<tr>
<td><strong>Secondary</strong></td>
<td>Secondary VLAN identifier.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Secondary VLAN type (community, isolated, or primary).</td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td>Ports which are associated with a private VLAN.</td>
</tr>
<tr>
<td><strong>VLAN ID</strong></td>
<td>The VLAN identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.</td>
</tr>
<tr>
<td><strong>VLAN Name</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>VLAN Type</strong></td>
<td>Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) if a RADIUS-assigned VLAN does not exist on the switch.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>slot/port. It is possible to set the parameters for all ports by using the selectors on the top line.</td>
</tr>
<tr>
<td><strong>Current</strong></td>
<td>The degree of participation of this port in this VLAN. The permissible values are:</td>
</tr>
<tr>
<td><strong>Configured</strong></td>
<td>The configured degree of participation of this port in this VLAN. The permissible values are:</td>
</tr>
<tr>
<td><strong>Tagging</strong></td>
<td>The tagging behavior for this port in this VLAN.</td>
</tr>
<tr>
<td><strong>Base VLAN ID</strong></td>
<td>Identifies the base VLAN ID for Internal allocation of VLANs to the routing interface.</td>
</tr>
<tr>
<td><strong>Allocation policy</strong></td>
<td>Identifies whether the system allocates VLAN IDs in ascending or descending order.</td>
</tr>
</tbody>
</table>
4.4.29  show vlan brief

This command displays a list of all configured VLANs.

Format  

show vlan brief

Mode  

• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>There is a VLAN Identifier (vlanid) associated with each VLAN. The range of</td>
</tr>
<tr>
<td></td>
<td>the VLAN ID is 1 to 4093.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>A string associated with this VLAN as a convenience. It can be up to 32</td>
</tr>
<tr>
<td></td>
<td>alphanumeric characters long, including blanks. The default is blank. VLAN</td>
</tr>
<tr>
<td></td>
<td>ID 1 always has a name of “Default.” This field is optional.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is</td>
</tr>
<tr>
<td></td>
<td>configured and permanently defined), or a Dynamic (one that is created by</td>
</tr>
<tr>
<td></td>
<td>GVRP registration).</td>
</tr>
</tbody>
</table>

4.4.30  show vlan port

This command displays VLAN port information.

Format  

show vlan port {slot/port | all}

Mode  

• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port It is possible to set the parameters for all ports by using the</td>
</tr>
<tr>
<td></td>
<td>selectors on the top line.</td>
</tr>
<tr>
<td>Port VLAN ID</td>
<td>The VLAN ID that this port will assign to untagged frames or priority</td>
</tr>
<tr>
<td>Configured</td>
<td>tagged frames received on this port. The value must be for an existing VLAN.</td>
</tr>
<tr>
<td>Port VLAN ID</td>
<td>The current VLAN ID that this port assigns to untagged frames or priority</td>
</tr>
<tr>
<td>Current</td>
<td>tagged frames received on this port. The factory default is 1.</td>
</tr>
<tr>
<td>Acceptable Frame</td>
<td>The types of frames that may be received on this port. The options are ‘VLAN</td>
</tr>
<tr>
<td>Types</td>
<td>only’ and ‘Admit All’. When set to ‘VLAN only’, untagged frames or priority</td>
</tr>
<tr>
<td></td>
<td>tagged frames received on this port are discarded. When set to ‘Admit All’,</td>
</tr>
<tr>
<td></td>
<td>untagged frames or priority tagged frames received on this port are</td>
</tr>
<tr>
<td></td>
<td>accepted and assigned the value of the Port VLAN ID for this port.</td>
</tr>
<tr>
<td></td>
<td>With either option, VLAN tagged frames are forwarded in accordance to the</td>
</tr>
<tr>
<td></td>
<td>802.1Q VLAN specification.</td>
</tr>
<tr>
<td>Ingress Filtering</td>
<td>May be enabled or disabled. When enabled, the frame is discarded if this</td>
</tr>
<tr>
<td>Configured</td>
<td>port is not a member of the VLAN with which this frame is associated. In</td>
</tr>
<tr>
<td>Current</td>
<td>a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an</td>
</tr>
<tr>
<td></td>
<td>untagged frame, the VLAN is the Port VLAN ID specified for the port that</td>
</tr>
<tr>
<td></td>
<td>received this frame. When disabled, all frames are forwarded in accordance</td>
</tr>
<tr>
<td></td>
<td>with the 802.1Q VLAN bridge specification. The factory default is disabled.</td>
</tr>
<tr>
<td>Ingress Filtering</td>
<td>Shows the current ingress filtering configuration.</td>
</tr>
<tr>
<td>Current</td>
<td>May be enabled or disabled.</td>
</tr>
<tr>
<td>GVRP</td>
<td>The 802.1p priority assigned to tagged packets arriving on the port.</td>
</tr>
<tr>
<td>Protected Port</td>
<td>Specifies if this is a protected port. If False, it is not a protected</td>
</tr>
<tr>
<td>Switchport mode</td>
<td>port; If true, it is.</td>
</tr>
<tr>
<td>Operating parameters</td>
<td>The operating parameters for the port, including the VLAN, name, egress</td>
</tr>
<tr>
<td></td>
<td>rule, and type.</td>
</tr>
<tr>
<td>Static configuration</td>
<td>The static configuration for the port, including the VLAN, name, and egress</td>
</tr>
<tr>
<td>Forbidden VLANs</td>
<td>The forbidden VLAN configuration for the port, including the VLAN and name.</td>
</tr>
</tbody>
</table>
4.4.31  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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address assigned to each interface.</td>
</tr>
<tr>
<td>Net Mask</td>
<td>The subnet mask.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>There is a VLAN Identifier (VID) associated with each VLAN.</td>
</tr>
</tbody>
</table>

4.4.32  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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Address</td>
<td>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.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>There is a VLAN Identifier (VID) associated with each VLAN.</td>
</tr>
</tbody>
</table>

4.5  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 IEEE 802.1Q domain.

4.5.1  dvlan-tunnel ethertype (Interface Config)

This command is not available on all platforms.

This command configures the ethertype for the specified interface. The two-byte hex ethertype is used as the first 16 bits of the DVLAN tag. The ethertype may have the values of 802.1Q, vman, or custom. If the ethertype has an optional value of custom, then it is a custom tunnel value, and ethertype must be set to a value in the range of 1 to 65535.

Default  vman
Format    dvlan-tunnel ethertype {802.1Q | vman | custom 1-65535}
Mode      Global Config
4.5.1.1  no dvlan-tunnel ethertype (Interface Config)

This command removes the ethertype value for the interface.

**Format**

```
no dvlan-tunnel ethertype
```

**Mode**

Global Config

### 4.5.2  dvlan-tunnel ethertype primary-tpid

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

**Format**

```
dvlan-tunnel ethertype {802.1Q | vman | custom 1-65535} [primary-tpid]
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q</td>
<td>Configure the ethertype as 0x8100.</td>
</tr>
<tr>
<td>custom</td>
<td>Configure the value of the custom tag in the range from 1 to 65535.</td>
</tr>
<tr>
<td>vman</td>
<td>Represents the commonly used value of 0x88A8.</td>
</tr>
</tbody>
</table>

4.5.2.1  no dvlan-tunnel ethertype primary–tpid

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

**Format**

```
no dvlan-tunnel ethertype {802.1Q | vman | custom 1-65535} [primary-tpid]
```

**Mode**

Global Config

**4.5.3  mode dot1q-tunnel**

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

**Default**

disabled

**Format**

```
mode dot1q-tunnel
```

**Mode**

Interface Config
4.5.3.1  no mode dot1q-tunnel
This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

**Format**  
no mode dot1q-tunnel

**Mode**  
Interface Config

4.5.4  mode dvlan-tunnel
Use this command to enable Double VLAN Tunneling on the specified interface.

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

**Default**  
disabled

**Format**  
mode dvlan-tunnel

**Mode**  
Interface Config

4.5.4.1  no mode dvlan-tunnel
This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

**Format**  
no mode dvlan-tunnel

**Mode**  
Interface Config

4.5.5  show dot1q-tunnel
Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

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

**Mode**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>slot/port</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.</td>
</tr>
<tr>
<td><strong>EtherType</strong></td>
<td>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 1 to 65535.</td>
</tr>
</tbody>
</table>
4.5.6  show dvlan-tunnel

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

Format  show dvlan-tunnel [interface {slot/port|all|lag lag_intf-num}]

Mode    •  Privileged EXEC
         •  User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>LAG</td>
<td>Instead of slot/port, lag lag_intf-num can be used as an alternate way to specify the LAG interface. lag lag_intf-num can also be used to specify the LAG interface where lag_intf-num is the LAG port number.</td>
</tr>
<tr>
<td>Mode</td>
<td>The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.</td>
</tr>
<tr>
<td>EtherType</td>
<td>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 1 to 65535.</td>
</tr>
</tbody>
</table>

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

(Routing) #show dvlan-tunnel

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

(Fastpath Routing) #

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

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

4.6  Private VLAN Commands

This section describes the commands you use for private VLANs. Private VLANs provides Layer 2 isolation between ports that share the same broadcast domain. In other words, it allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network.

4.6.1  switchport private-vlan

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Format  switchport private-vlan {host-association primary-vlan-id secondary-vlan-id | mapping primary-vlan-id {add | remove} secondary-vlan-list}

Mode    Interface Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-association</td>
<td>Defines the VLAN association for community or host ports.</td>
</tr>
<tr>
<td>mapping</td>
<td>Defines the private VLAN mapping for promiscuous ports.</td>
</tr>
</tbody>
</table>
4.6.1 no switchport private-vlan
This command removes the private-VLAN association or mapping from the port.

Format: no switchport private-vlan {host-association|mapping}
Mode: Interface Config

4.6.2 switchport mode private-vlan
This command configures a port as a promiscuous or host private VLAN port. Note that the properties of each mode can be configured even when the switch is not in that mode. However, they will only be applicable once the switch is in that particular mode.

Default: general

Format: switchport mode private-vlan {host|promiscuous}
Mode: Interface Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Configures an interface as a private VLAN host port. It can be either isolated or community port depending on the secondary VLAN it is associated with.</td>
</tr>
<tr>
<td>promiscuous</td>
<td>Configures an interface as a private VLAN promiscuous port. The promiscuous ports are members of the primary VLAN.</td>
</tr>
</tbody>
</table>

4.6.2.1 no switchport mode private-vlan
This command removes the private-VLAN association or mapping from the port.

Format: no switchport mode private-vlan
Mode: Interface Config

4.6.3 private-vlan
This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format: private-vlan {association [add|remove] secondary-vlan-list|community|isolated|primary}
Mode: VLAN Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>association</td>
<td>Associates the primary and secondary VLAN.</td>
</tr>
<tr>
<td>secondary-vlan-list</td>
<td>A list of secondary VLANs to be mapped to a primary VLAN.</td>
</tr>
</tbody>
</table>
4.6.3.1 no private-vlan
This command restores normal VLAN configuration.

Format: no private-vlan {association}
Mode: VLAN Config

4.7 Switch Ports
This section describes the commands used for switch port mode.

4.7.1 switchport mode
Use this command to configure the mode of a switch port as access, trunk or general.

In Trunk mode, the port becomes a member of all VLANs on switch unless specified in the allowed list in the switchport trunk allowed vlan command. The PVID of the port is set to the Native VLAN as specified in the switchport trunk native vlan command. It means that trunk ports accept both tagged and untagged packets, where untagged packets are processed on the native VLAN and tagged packets are processed on the VLAN ID contained in the packet. MAC learning is performed on both tagged and untagged packets. Tagged packets received with a VLAN ID of which the port is not a member are discarded and MAC learning is not performed. The Trunk ports always transmit packets untagged on native VLAN.

In Access mode, the port becomes a member of only one VLAN. The port sends and receives untagged traffic. It can also receive tagged traffic. The ingress filtering is enabled on port. It means that when the VLAN ID of received packet is not identical to Access VLAN ID, the packet is discarded.

In General mode, the user can perform custom configuration of VLAN membership, PVID, tagging, ingress filtering etc. This is legacy FASTPATH behavior of switch port configuration. Legacy FASTPATH CLI commands are used to configure port in general mode.

Default: General mode
Format: switchport mode {access | trunk | general}
Mode: Interface Config

4.7.1.1 no switchport mode
This command resets the switch port mode to its default value.

Format: no switchport mode
Mode: Interface Config

4.7.2 switchport trunk allowed vlan
Use this command to configure the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. The default is all.

The VLANs list can be modified using the add or remove options or replaced with another list using the vlan-list, all, or except options. If all is chosen, all VLANs are added to the list of allowed vlan. The except option provides an exclusion list.

Trunk ports accept tagged packets, where tagged packets are processed on the VLAN ID contained in the packet, if this VLAN is in the allowed VLAN list. Tagged packets received with a VLAN ID to which the port is not a member are discarded and MAC learning is not performed. If a VLAN is added to the system after a port is set to the Trunk mode and it is in the allowed VLAN list, this VLAN is assigned to this port automatically.
4.7.2.1 no switchport trunk allowed vlan

This command resets the list of allowed VLANs on the trunk port to its default value.

Format
no switchport trunk allowed vlan

Mode
Interface Config

4.7.3 switchport trunk native vlan

Use this command to configure the Trunk port Native VLAN (PVID) parameter. Any ingress untagged packets on the port are tagged with the value of Native VLAN. Native VLAN must be in the allowed VLAN list for tagging of received untagged packets. Otherwise, untagged packets are discarded. Packets marked with Native VLAN are transmitted untagged from Trunk port. The default is 1.

Default
1 (Default VLAN)

Format
switchport trunk native vlan vlan-id

Mode
Interface Config
4.7.3.1  no switchport trunk native vlan

Use this command to reset the switch port trunk mode native VLAN to its default value.

Format   no switchport trunk native vlan
Mode     Interface Config

4.7.4  switchport access vlan

Use this command to configure the VLAN on the Access port. Only one VLAN can be assigned to the Access port. Access ports are members of VLAN 1 by default. Access ports may be assigned to a VLAN other than VLAN 1. Removing the Access VLAN on the switch makes the Access port a member of VLAN 1. Configuring an Access port to be a member of a VLAN that does not exist results in an error and does not change the configuration.

Default   1 (Default VLAN)
Format    switchport access vlan vlan-id
Mode      Interface Config

4.7.4.1  no switchport access vlan

This command resets the switch port access mode VLAN to its default value.

Format    no switchport access vlan
Mode      Interface Config

4.7.5  show interfaces switchport

Use this command to display the switchport status for all interfaces or a specified interface.

Format    show interfaces switchport slot/port
Mode      Privileged EXEC

Example:
(Routing) #show interfaces switchport 0/1

Port: 0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANS:
General Mode Untagged VLANS: 1
General Mode Tagged VLANS:
General Mode Forbidden VLANS:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False

(Routing) #show interfaces switchport

Port: 0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False

4.7.6 show interfaces switchport
Use this command to display the Switchport configuration for a selected mode per interface. If the interface is not specified, the configuration for all interfaces is displayed.

Format: show interfaces switchport {access | trunk | general} [slot/port]
Mode: Privileged EXEC

Example:
(Switching) # show interfaces switchport access 0/1

<table>
<thead>
<tr>
<th>Intf</th>
<th>PVID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>1</td>
</tr>
</tbody>
</table>

(Switching) # show interfaces switchport trunk 0/6

<table>
<thead>
<tr>
<th>Intf</th>
<th>PVID</th>
<th>Allowed Vlans List</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/6</td>
<td>1</td>
<td>All</td>
</tr>
</tbody>
</table>

(Switching) # show interfaces switchport general 0/5

<table>
<thead>
<tr>
<th>Intf</th>
<th>PVID</th>
<th>Ingress Filtering</th>
<th>Acceptable Frame Type</th>
<th>Untagged VLANs</th>
<th>Tagged VLANs</th>
<th>Forbidden VLANs</th>
<th>Dynamic Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/5</td>
<td>1</td>
<td>Enabled</td>
<td>Admit All</td>
<td>7</td>
<td>10-50,55</td>
<td>9,100-200</td>
<td>88,96</td>
</tr>
</tbody>
</table>

(Switching) # show interfaces switchport general

<table>
<thead>
<tr>
<th>Intf</th>
<th>PVID</th>
<th>Ingress Filtering</th>
<th>Acceptable Frame Type</th>
<th>Untagged VLANs</th>
<th>Tagged VLANs</th>
<th>Forbidden VLANs</th>
<th>Dynamic Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>1</td>
<td>Enabled</td>
<td>Admit All</td>
<td>1,4-7</td>
<td>30-40,55</td>
<td>3,100-200</td>
<td>88,96</td>
</tr>
<tr>
<td>0/2</td>
<td>1</td>
<td>Disabled</td>
<td>Admit All</td>
<td>1</td>
<td>30-40,55</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

4.8 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.
4.8.1 voice vlan (Global Config)
Use this command to enable the Voice VLAN capability on the switch.

Default: disabled

Format: voice vlan

Mode: Global Config

4.8.1.1 no voice vlan (Global Config)
Use this command to disable the Voice VLAN capability on the switch.

Format: no voice vlan

Mode: Global Config

4.8.2 voice vlan (Interface Config)
Use this command to enable the Voice VLAN capability on the interface or range of interfaces.

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>Configure the IP phone to forward all voice traffic through the specified VLAN. Valid VLAN ID’s are from 1 to 4093 (the max supported by the platform).</td>
</tr>
<tr>
<td>dot1p</td>
<td>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.</td>
</tr>
<tr>
<td>none</td>
<td>Allow the IP phone to use its own configuration to send untagged voice traffic.</td>
</tr>
<tr>
<td>untagged</td>
<td>Configure the phone to send untagged voice traffic.</td>
</tr>
</tbody>
</table>

4.8.2.1 no voice vlan (Interface Config)
Use this command to disable the Voice VLAN capability on the interface.

Format: no voice vlan

Mode: Interface Config

4.8.3 voice vlan data priority
Use this command to either trust or untrust the data traffic arriving on the Voice VLAN interface or range of interfaces being configured.

Default: trust

Format: voice vlan data priority {untrust | trust}

Mode: Interface Config
4.8.4 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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Mode</td>
<td>The Global Voice VLAN mode.</td>
</tr>
</tbody>
</table>

When the `interface` is specified:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice VLAN Mode</td>
<td>The admin mode of the Voice VLAN on the interface.</td>
</tr>
<tr>
<td>Voice VLAN ID</td>
<td>The Voice VLAN ID</td>
</tr>
<tr>
<td>Voice VLAN Priority</td>
<td>The d01p priority for the Voice VLAN on the port.</td>
</tr>
<tr>
<td>Voice VLAN Untagged</td>
<td>The tagging option for the Voice VLAN traffic.</td>
</tr>
<tr>
<td>Voice VLAN CoS Override</td>
<td>The Override option for the voice traffic arriving on the port.</td>
</tr>
<tr>
<td>Voice VLAN Status</td>
<td>The operational status of Voice VLAN on the port.</td>
</tr>
</tbody>
</table>

4.9 Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

4.9.1 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

4.9.2 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
4.10 Asymmetric Flow Control

Asymmetric Flow Control can only be configured globally for all ports on XGS4 silicon-based switches.

Asymmetric Flow Control is not supported on Fast Ethernet platforms.

If Asymmetric Flow Control is not supported on the platform, then only symmetric, or no flow control, modes are configurable.

When in asymmetric flow control mode, the switch responds to PAUSE frames received from a peer by stopping packet transmission, but the switch does not initiate MAC control PAUSE frames.
When you configure the switch in asymmetric flow control (or no flow control mode), the device is placed in egress drop mode. Egress drop mode maximizes the throughput of the system at the expense of packet loss in a heavily congested system, and this mode avoids head-of-line blocking.

4.10.1 flowcontrol {symmetric|asymmetric}

The flowcontrol {symmetric|asymmetric} command is available if the platform supports the asymmetric flow control feature.

Use this command to enable or disable the symmetric or asymmetric flow control on the switch. Asymmetric here means that Tx Pause can never be enabled. Only Rx Pause can be enabled.

Default Flow control is disabled.

Format flowcontrol {symmetric|asymmetric}

Mode Global Config

4.10.1.1 no flowcontrol {symmetric|asymmetric}

Use the no form of this command to disable symmetric or asymmetric flow control.

Format no flowcontrol {symmetric|asymmetric}

Mode Global Config

4.10.2 flowcontrol

This flowcontrol command is available if the platform supports only the symmetric flow control feature.

Use this command to enable or disable the symmetric flow control on the switch.

Default Flow control is disabled.

Format flowcontrol

Mode Global Config
4.10.2.1 no flowcontrol
Use the no form of this command to disable the symmetric flow control.

Format  no flowcontrol
Mode    Global Config

4.10.3 show flowcontrol
Use this command to display the IEEE 802.3 Annex 31B flow control settings and status for a specific interface or all interfaces. The command also displays 802.3 Tx and Rx pause counts. Priority Flow Control frames counts are not displayed. If the port is enabled for priority flow control, operational flow control status is displayed as Inactive. Operational flow control status for stacking ports is always displayed as N/A.

Format  show flowcontrol [slot/port]
Mode    Privileged EXEC

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

(Switching)#show flowcontrol
Admin Flow Control: Symmetric

Port Flow Control RxPause TxPause
------- --------- ------- -------
0/1 Active 310 611
0/2 Inactive 0 0

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

(Switching)#show flowcontrol interface 0/1
Admin Flow Control: Symmetric

Port Flow Control RxPause TxPause
------- --------- ------- -------
0/1 Active 310 611

4.11 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.

4.11.1 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.

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.
4.11.1 no switchport protected (Global Config)
Use this command to remove a protected port group. The `groupid` parameter identifies the set of protected ports. The `name` keyword specifies the name to remove from the group.

**Format**
```
no switchport protected groupid name
```

**Mode**
Global Config

4.11.2 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.

**Format**
```
switchport protected groupid
```

**Mode**
Interface Config

4.11.2.1 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

4.11.3 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

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>The number that identifies the protected port group.</td>
</tr>
<tr>
<td>Name</td>
<td>An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.</td>
</tr>
<tr>
<td>List of Physical Ports</td>
<td>List of ports, which are configured as protected for the group identified with <code>groupid</code>. If no port is configured as protected for this group, this field is blank.</td>
</tr>
</tbody>
</table>
4.11.4 **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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Protected</td>
<td>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 <code>groupid</code></td>
</tr>
</tbody>
</table>

### 4.12 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 GVRP) or multicast groups (by using GMRP).

#### 4.12.1 set garp timer join

This command sets the GVRP join time per GARP for one interface, a range of interfaces, or all interfaces. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or reregistering) 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

#### 4.12.1.1 no set garp timer join

This command sets the GVRP join time to the default and only has an effect when GVRP is enabled.

**Format**

```
no set garp timer join
```

**Mode**

- Interface Config
- Global Config

#### 4.12.2 set garp timer leave

This command sets the GVRP leave time for one interface, a range of interfaces, or all interfaces or all ports 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. The leave time must be greater than or equal to three times the join time.

**Default**

60

**Format**

```
set garp timer leave 20-600
```

**Mode**

- Interface Config
- Global Config
4.12.2.1 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

4.12.3 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 on a single port or a range of ports (Interface Config mode) and it only has an effect only when GVRP is enabled. The leave all time must be greater than the leave time.

**Default**

```
1000
```

**Format**

```
set garp timer leaveall 200-6000
```

**Mode**

- Interface Config
- Global Config

4.12.3.1 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

4.12.4 show garp

This command displays GARP information.

**Format**

```
show garp
```

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMRP Admin Mode</td>
<td>The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.</td>
</tr>
<tr>
<td>GVRP Admin Mode</td>
<td>The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.</td>
</tr>
</tbody>
</table>

4.13 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.

---

**NOTICE**

If GVRP is disabled, the system does not forward GVRP messages.
4.13.1 set gvrp adminmode
This command enables GVRP on the system.

Default: disabled
Format: set gvrp adminmode
Mode: Privileged EXEC

4.13.1.1 no set gvrp adminmode
This command disables GVRP.

Format: no set gvrp adminmode
Mode: Privileged EXEC

4.13.2 set gvrp interfacemode
This command enables GVRP on a single port (Interface Config mode), a range of ports (Interface Range mode), or all ports (Global Config mode).

Default: disabled
Format: set gvrp interfacemode
Mode:
  • Interface Config
  • Interface Range
  • Global Config

4.13.2.1 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

4.13.3 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interval between the transmission of GARP PDUs registering (or reregistering) 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).</td>
</tr>
</tbody>
</table>
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.

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

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

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

---

### 4.14 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.

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

### 4.14.1 set gmrp adminmode

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

**Default** disabled  
**Format** `set gmrp adminmode`  
**Mode** Privileged EXEC

### 4.14.1.1 no set gmrp adminmode

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

**Format** `no set gmrp adminmode`  
**Mode** Privileged EXEC

### 4.14.2 set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode), a range of interfaces, 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
4.14.2.1 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

4.14.3 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The slot/port of the interface that this row in the table describes.</td>
</tr>
<tr>
<td>Join Timer</td>
<td>The interval between the transmission of GARP PDUs registering (or reregistering) 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).</td>
</tr>
<tr>
<td>Leave Timer</td>
<td>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).</td>
</tr>
<tr>
<td>LeaveAll Timer</td>
<td>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).</td>
</tr>
<tr>
<td>Port GMRP Mode</td>
<td>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.</td>
</tr>
</tbody>
</table>

4.14.4 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN in which the MAC Address is learned.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.</td>
</tr>
<tr>
<td>Type</td>
<td>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.</td>
</tr>
</tbody>
</table>
4.15 Port-Based Network Access Control Commands

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

4.15.1 aaa authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- ias. Uses the internal authentication server users database for authentication. This method can be used in conjunction with any one of the existing methods like local, radius, etc.
- local. Uses the local username database for authentication.
- none. Uses no authentication.
- radius. Uses the list of all RADIUS servers for authentication.

**Example:** The following is an example of the command.

```
(FASTPATH Routing) #
(FASTPATH Routing) (Config)#aaa authentication dot1x default ias none
```

4.15.2 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

4.15.3 clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

**Format**

```
clear dot1x authentication-history [slot/port]
```

**Mode**

Privileged EXEC

4.15.4 clear radius statistics

This command is used to clear all RADIUS statistics.

**Format**

```
clear radius statistics
```

**Mode**

Privileged EXEC
4.15.5  **dot1x eapolflood**
Use this command to enable EAPOL flood support on the switch.

*Default*  disabled

*Format*  dot1x eapolflood

*Mode*  Global Config

4.15.5.1  **no dot1x eapolflood**
This command disables EAPOL flooding on the switch.

*Format*  no dot1x eapolflood

*Mode*  Global Config

4.15.6  **dot1x dynamic-vlan enable**
Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

*Default*  Disabled

*Format*  dot1x dynamic-vlan enable

*Mode*  Global Config

4.15.6.1  **no dot1x dynamic-vlan enable**
Use this command to prevent the switch from creating VLANs when a RADIUS-assigned VLAN does not exist in the switch.

*Format*  no dot1x dynamic-vlan enable

*Mode*  Global Config

4.15.7  **dot1x guest-vlan**
This command configures VLAN as guest vlan on an interface or a range of interfaces. 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
4.15.7.1 no dot1x guest-vlan
This command disables Guest VLAN on the interface.

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

4.15.8 dot1x initialize
This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format: dot1x initialize slot/port
Mode: Privileged EXEC

4.15.9 dot1x max-req
This command sets the maximum number of times the authenticator state machine on an interface or range of interfaces 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

4.15.9.1 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

4.15.10 dot1x max-users
Use this command to set the maximum number of clients supported on an interface or range of interfaces 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 - 48.

Default: 48
Format: dot1x max-users count
Mode: Interface Config
4.15.10  no dot1x max-users
This command resets the maximum number of clients allowed per port to its default value.

Format    no dot1x max-users
Mode      Interface Config

4.15.11  dot1x port-control
This command sets the authentication mode to use on the specified interface or range of interfaces. Use the force-unauthorized parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the force-authorized parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the auto parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

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

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

4.15.11.1  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

4.15.12  dot1x port-control all
This command sets the authentication mode to use on all ports. Select force-unauthorized to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select force-authorized to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select auto to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

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

Default  auto
Format    dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}
Mode      Global Config
4.15.12  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

4.15.13  dot1x mac-auth-bypass
If the 802.1X mode on the interface is mac-based, you can optionally use this command to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients – such as printers, fax machines, and some IP phones — to authenticate to the network using the client MAC address as an identifier.

**Default**  
disabled

**Format**  
dot1x mac-auth-bypass

**Mode**  
Interface Config

4.15.13.1  no dot1x mac-auth-bypass
This command sets the MAB mode on the ports to the default value.

**Format**  
no dot1x mac-auth-bypass

**Mode**  
Interface Config

4.15.14  dot1x re-authenticate
This command begins the reauthentication sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

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

**Mode**  
Privileged EXEC

4.15.15  dot1x re-authentication
This command enables reauthentication of the supplicant for the specified interface or range of interfaces.

**Default**  
disabled

**Format**  
dot1x re-authentication

**Mode**  
Interface Config

---

**NOTICE**  
MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.
4.15.15.1  **no dot1x re-authentication**
This command disables reauthentication of the supplicant for the specified port.

<table>
<thead>
<tr>
<th>Format</th>
<th>no dot1x re-authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

4.15.16  **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.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>dot1x system-auth-control</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.15.16.1 **no dot1x system-auth-control**
This command is used to disable the dot1x authentication support on the switch.

<table>
<thead>
<tr>
<th>Format</th>
<th>no dot1x system-auth-control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.15.17  **dot1x system-auth-control monitor**
Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help trouble-shoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>dot1x system-auth-control monitor</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.15.17.1 **no dot1x system-auth-control monitor**
This command disables the 802.1X Monitor mode on the switch.

<table>
<thead>
<tr>
<th>Format</th>
<th>no dot1x system-auth-control monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>
4.15.18  dot1x timeout

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

<table>
<thead>
<tr>
<th>Tokens</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest-vlan-period</td>
<td>The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.</td>
</tr>
<tr>
<td>reauth-period</td>
<td>The value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.</td>
</tr>
<tr>
<td>quiet-period</td>
<td>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.</td>
</tr>
<tr>
<td>tx-period</td>
<td>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.</td>
</tr>
<tr>
<td>supp-timeout</td>
<td>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.</td>
</tr>
<tr>
<td>server-timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

4.15.18.1  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

4.15.19  dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface or range of interfaces. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (4093 for FASTPATH). 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.

Default

0

Format
dot1x unauthenticated-vlan vlan id

Mode Interface Config
4.15.19.1  no dot1x unauthenticated-vlan
This command resets the unauthenticated-vlan associated with the port to its default value.

Format  no dot1x unauthenticated-vlan
Mode     Interface Config

4.15.20   dot1x user
This command adds the specified user to the list of users with access to the specified port or all ports. The user parameter must be a configured user.

Format  dot1x user user {slot/port | all}
Mode     Global Config

4.15.20.1  no dot1x user
This command removes the user from the list of users with access to the specified port or all ports.

Format  no dot1x user user {slot/port | all}
Mode     Global Config

4.15.21   authentication enable
This command globally enables the Authentication Manager. Interface configuration takes effect only if the Authentication Manager is enabled with this command.

Default   disabled
Format     authentication enable
Mode       Global Config

4.15.21.1  no authentication enable
This command disables the Authentication Manager.

Format     no authentication enable
Mode       Global Config

4.15.22   authentication order
This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Mode     Interface Config
4.15.22.1  no authentication order

This command returns the port to the default authentication order.

Format:  no authentication order
Mode:    Interface Config

4.15.23  authentication priority

This command sets the priority for the authentication methods used on a port. The available authentication methods are
Dot1x, MAB, and captive portal. The authentication priority decides if a previously authenticated client is reauthenticated
with a higher-priority method when the same is received. Captive portal is always the last method in the list.

Default:  authentication order dot1x mab captive portal
Format:   authentication priority {dot1x mab captive portal} | captive portal | mab {dot1x captive portal} | captive portal
Mode:     Interface Config

4.15.23.1  no authentication priority

This command returns the port to the default order of priority for the authentication methods.

Format:   no authentication priority
Mode:     Interface Config

4.15.24  authentication timer restart

This command sets the time, in seconds, after which reauthentication starts. (The default time is 300 seconds.) The
timer restarts the authentication only after all the authentication methods fail. At the expiration of this timer, authenti-
cation is reinitiated for the port.

Format:   authentication timer restart <300-65535>
Mode:     Interface Config

4.15.24.1  no authentication timer restart

This command sets the reauthentication value to the default value of 3600 seconds.

Format:   no authentication timer restart
Mode:     Interface Config

4.15.25  show authentication authentication-history

Use this command to display information about the authentication history for a specified interface.

Format:   show authentication authentication-history slot/port
Mode:     Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Stamp</td>
<td>The time of the authentication.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface.</td>
</tr>
<tr>
<td>MAC-Address</td>
<td>The MAC address for the interface.</td>
</tr>
</tbody>
</table>
**Auth Status Method**
The authentication method and status for the interface.

---

**Example:** The following information is shown for the interface.

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Interface</th>
<th>MAC-Address</th>
<th>Auth Status</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 21 1919 15:06:15</td>
<td>0/1</td>
<td>00:00:00:00:00:01</td>
<td>Authorized</td>
<td>802.1X</td>
</tr>
</tbody>
</table>

### 4.15.26 show authentication interface

Use this command to display authentication method information either for all interfaces or a specified port.

**Format**

```
show authentication interface {all | slot/port }
```

**Mode**

Privileged EXEC

The following information is displayed for each interface.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface for which authentication configuration information is being displayed.</td>
</tr>
<tr>
<td>Authentication Restart timer</td>
<td>The time, in seconds, after which reauthentication starts.</td>
</tr>
<tr>
<td>Configured method order</td>
<td>The order of authentication methods used on a port.</td>
</tr>
<tr>
<td>Enabled method order</td>
<td>The order of authentication methods used on a port.</td>
</tr>
<tr>
<td>Configured method priority</td>
<td>The priority for the authentication methods used on a port.</td>
</tr>
<tr>
<td>Enabled method priority</td>
<td>The priority for the authentication methods used on a port.</td>
</tr>
<tr>
<td>Number of authenticated clients</td>
<td>The number of authenticated clients.</td>
</tr>
<tr>
<td>Logical Interface</td>
<td>The logical interface</td>
</tr>
<tr>
<td>Client MAC addr</td>
<td>The MAC address for the client.</td>
</tr>
<tr>
<td>Authenticated Method</td>
<td>The current authentication method.</td>
</tr>
<tr>
<td>Auth State</td>
<td>If the authentication was successful.</td>
</tr>
<tr>
<td>Auth Status</td>
<td>The current authentication status.</td>
</tr>
</tbody>
</table>

**Example:** The following example displays the authentication interface information for all interfaces.

```
(switch) #show authentication interface all

Interface...................................... 0/1
Authentication Restart timer............. 300
Configured method order.................... dot1x mab captive-portal
Enabled method order....................... dot1x mab undefined
Configured method priority................ undefined undefined undefined
Enabled method priority.................... undefined undefined undefined
Number of authenticated clients.......... 0
Interface...................................... 0/2
Authentication Restart timer............. 300
Configured method order.................... dot1x mab captive-portal
Enabled method order....................... dot1x mab undefined
Configured method priority................ undefined undefined undefined
Enabled method priority.................... undefined undefined undefined
Number of authenticated clients.......... 0
Interface...................................... 0/3
Authentication Restart timer............. 300
Configured method order.................... dot1x mab captive-portal
Enabled method order....................... dot1x mab undefined
Configured method priority................ undefined undefined undefined
```
Enabled method priority........................ undefined undefined undefined undefined
Number of authenticated clients................. 0
Interface...................................... 0/4
Authentication Restart timer.................... 300
Configured method order........................ dot1x mab captive-portal
Enabled method order......................... dot1x mab undefined
Configured method priority..................... undefined undefined undefined undefined
Enabled method priority........................ undefined undefined undefined undefined
Number of authenticated clients................. 0

4.15.27 show authentication methods

Use this command to display information about the authentication methods.

Format               show authentication methods
Mode                 Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Login List</td>
<td>The authentication login listname.</td>
</tr>
<tr>
<td>Method 1</td>
<td>The first method in the specified authentication login list, if any.</td>
</tr>
<tr>
<td>Method 2</td>
<td>The second method in the specified authentication login list, if any.</td>
</tr>
<tr>
<td>Method 3</td>
<td>The third method in the specified authentication login list, if any.</td>
</tr>
</tbody>
</table>

Example: The following example displays the authentication configuration.

(switch)#show authentication methods

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

Enable Authentication Method Lists
-----------------------------------
enableList    : enable  none
enableNetList : enable  deny

<table>
<thead>
<tr>
<th>Line</th>
<th>Login Method List</th>
<th>Enable Method List</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>defaultList</td>
<td>enableList</td>
</tr>
<tr>
<td>Telnet</td>
<td>networkList</td>
<td>enableNetList</td>
</tr>
<tr>
<td>SSH</td>
<td>networkList</td>
<td>enableNetList</td>
</tr>
</tbody>
</table>

HTTPS :local
HTTP :local
DOT1X :

4.15.28 show authentication statistics

Use this command to display the authentication statistics for an interface.

Format               show authentication statistics slot/port
Mode                 Privileged EXEC

The following information is displayed for each interface.
### 4.15.29 clear authentication statistics

Use this command to clear the authentication statistics on an interface.

**Format**
```
clear authentication authentication-history {slot/port | all}
```

**Mode** Privileged EXEC

### 4.15.30 clear authentication authentication-history

Use this command to clear the authentication history log for an interface.

**Format**
```
clear authentication authentication-history {slot/port | all}
```

**Mode** Privileged EXEC

### 4.15.31 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, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port for which information is being displayed.</td>
</tr>
<tr>
<td>802.1X attempts</td>
<td>The number of Dot1x authentication attempts for the port.</td>
</tr>
<tr>
<td>802.1X failed attempts</td>
<td>The number of failed Dot1x authentication attempts for the port.</td>
</tr>
<tr>
<td>Mab attempts</td>
<td>The number of MAB (MAC authentication bypass) authentication attempts for the port.</td>
</tr>
<tr>
<td>Mab failed attempts</td>
<td>The number of failed MAB authentication attempts for the port.</td>
</tr>
<tr>
<td>Captive-portal attempts</td>
<td>The number of captive portal (Web authorization) authentication attempts for the port.</td>
</tr>
<tr>
<td>Captive-portal failed attempts</td>
<td>The number of failed captive portal authentication attempts for the port.</td>
</tr>
</tbody>
</table>

_Example:_
(FASTPATH Routing) #show authentication statistics 0/1

Port........................................... 0/1
802.1X attempts.......................... 0
802.1X failed attempts................... 0
Mab attempts.................................. 0
Mab failed attempts....................... 0
Captive-portal attempts................... 0
Captive-portal failed attempts........... 0

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Mode</td>
<td>Indicates whether authentication control on the switch is enabled or disabled.</td>
</tr>
<tr>
<td>VLAN Assignment Mode</td>
<td>Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).</td>
</tr>
</tbody>
</table>
If you use the optional parameter `summary {slot/port | all}`, the dot1x configuration for the specified port or all ports are displayed.

**Example:** The following shows example CLI display output for the command `show dot1x summary 0/1`.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Control Mode</th>
<th>Operating Control Mode</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>auto</td>
<td>auto</td>
<td>Authorized</td>
</tr>
</tbody>
</table>

If you use the optional parameter `detail slot/port`, the detailed dot1x configuration for the specified port is displayed.

MAC-based dot1x authentication is supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Period</td>
<td>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.</td>
</tr>
<tr>
<td>Guest-VLAN ID</td>
<td>The guest VLAN identifier configured on the interface.</td>
</tr>
<tr>
<td>Guest VLAN Period</td>
<td>The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.</td>
</tr>
<tr>
<td>Supplicant Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Requests</td>
<td>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.</td>
</tr>
<tr>
<td>Configured MAB Mode</td>
<td>The administrative mode of the MAC authentication bypass feature on the switch.</td>
</tr>
<tr>
<td>Operational MAB Mode</td>
<td>The operational mode of the MAC authentication bypass feature on the switch. MAB might be administratively enabled but not operational if the control mode is not MAC-based.</td>
</tr>
<tr>
<td>Vlan-ID</td>
<td>The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not MAC-based.</td>
</tr>
<tr>
<td>VLAN Assigned Reason</td>
<td>The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.</td>
</tr>
<tr>
<td>Reauthentication Period</td>
<td>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.</td>
</tr>
<tr>
<td>Reauthentication Enabled</td>
<td>Indicates if reauthentication is enabled on this port. Possible values are ‘True’ or ‘False’.</td>
</tr>
<tr>
<td>Key Transmission Enabled</td>
<td>Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.</td>
</tr>
<tr>
<td>EAPOL Flood Mode Enabled</td>
<td>Indicates whether the EAPOL flood support is enabled on the switch. Possible values are True or False.</td>
</tr>
<tr>
<td>Control Direction</td>
<td>The control direction for the specified port or ports. Possible values are both or in.</td>
</tr>
<tr>
<td>Maximum Users</td>
<td>The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.</td>
</tr>
<tr>
<td>Unauthenticated VLAN ID</td>
<td>Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Session Termination Action</td>
<td>This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(switch) #show dot1x detail 0/3

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>0/1</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>1</td>
</tr>
<tr>
<td>PAE Capabilities</td>
<td>Authenticator</td>
</tr>
<tr>
<td>Control Mode</td>
<td>auto</td>
</tr>
<tr>
<td>Authenticator PAE State</td>
<td>Initialize</td>
</tr>
<tr>
<td>Backend Authentication State</td>
<td>Initialize</td>
</tr>
<tr>
<td>Quiet Period (secs)</td>
<td>60</td>
</tr>
<tr>
<td>Transmit Period (secs)</td>
<td>30</td>
</tr>
<tr>
<td>Guest VLAN ID</td>
<td>0</td>
</tr>
<tr>
<td>Guest VLAN Period (secs)</td>
<td>90</td>
</tr>
<tr>
<td>Supplicant Timeout (secs)</td>
<td>30</td>
</tr>
<tr>
<td>Server Timeout (secs)</td>
<td>30</td>
</tr>
<tr>
<td>Maximum Requests</td>
<td>2</td>
</tr>
<tr>
<td>Configured MAB Mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>Operational MAB Mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLAN Id</td>
<td>0</td>
</tr>
<tr>
<td>VLAN Assigned Reason</td>
<td>Not Assigned</td>
</tr>
<tr>
<td>Reauthentication Period (secs)</td>
<td>3600</td>
</tr>
<tr>
<td>Reauthentication Enabled</td>
<td>FALSE</td>
</tr>
<tr>
<td>Key Transmission Enabled</td>
<td>FALSE</td>
</tr>
<tr>
<td>EAPOL flood Mode Enabled</td>
<td>FALSE</td>
</tr>
<tr>
<td>Control Direction</td>
<td>both</td>
</tr>
<tr>
<td>Maximum Users</td>
<td>16</td>
</tr>
<tr>
<td>Unauthenticated VLAN ID</td>
<td>0</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>0</td>
</tr>
<tr>
<td>Session Termination Action</td>
<td>Default</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplicant MAC-Address</td>
<td>The MAC-address of the supplicant.</td>
</tr>
<tr>
<td>Authenticator PAE State</td>
<td>Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.</td>
</tr>
<tr>
<td>Backend Authentication State</td>
<td>Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.</td>
</tr>
<tr>
<td>VLAN-Assigned</td>
<td>The VLAN assigned to the client by the radius server.</td>
</tr>
<tr>
<td>Logical Port</td>
<td>The logical port number associated with the client.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The interface whose statistics are displayed.</td>
</tr>
<tr>
<td>EAPOL Frames Received</td>
<td>The number of valid EAPOL frames of any type that have been received by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Frames Transmitted</td>
<td>The number of EAPOL frames of any type that have been transmitted by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Start Frames Received</td>
<td>The number of EAPOL start frames that have been received by this authenticator.</td>
</tr>
</tbody>
</table>
4.15.32 show dot1x authentication-history

This command displays 802.1X authentication events and information during successful and unsuccessful Dot1x authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

**Format**

```
show dot1x authentication-history {slot/port | all} [failed-auth-only] [detail]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAPOL Logoff Frames Received</td>
<td>The number of EAPOL logoff frames that have been received by this authenticator.</td>
</tr>
<tr>
<td>Last EAPOL Frame Version</td>
<td>The protocol version number carried in the most recently received EAPOL frame.</td>
</tr>
<tr>
<td>Last EAPOL Frame Source</td>
<td>The source MAC address carried in the most recently received EAPOL frame.</td>
</tr>
<tr>
<td>EAP Response/Id Frames Received</td>
<td>The number of EAP response/identity frames that have been received by this authenticator.</td>
</tr>
<tr>
<td>EAP Response Frames Received</td>
<td>The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.</td>
</tr>
<tr>
<td>EAP Request/Id Frames Transmitted</td>
<td>The number of EAP request/identity frames that have been transmitted by this authenticator.</td>
</tr>
<tr>
<td>EAP Request Frames Transmitted</td>
<td>The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.</td>
</tr>
<tr>
<td>Invalid EAPOL Frames Received</td>
<td>The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.</td>
</tr>
<tr>
<td>EAP Length Error Frames Received</td>
<td>The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.</td>
</tr>
</tbody>
</table>

4.15.33 show dot1x clients

This command displays 802.1X client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

**Format**

```
show dot1x clients {slot/port | all}
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Stamp</td>
<td>The exact time at which the event occurs.</td>
</tr>
<tr>
<td>Interface</td>
<td>Physical Port on which the event occurs.</td>
</tr>
<tr>
<td>Mac-Address</td>
<td>The supplicant/client MAC address.</td>
</tr>
<tr>
<td>VLAN assigned</td>
<td>The VLAN assigned to the client/port on authentication.</td>
</tr>
<tr>
<td>VLAN assigned Reason</td>
<td>The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Monitor Mode VLAN ID.</td>
</tr>
<tr>
<td>Auth Status</td>
<td>The authentication status.</td>
</tr>
<tr>
<td>Reason</td>
<td>The actual reason behind the successful or failed authentication.</td>
</tr>
</tbody>
</table>
4.15.34 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Users configured locally to have access to the specified port.</td>
</tr>
</tbody>
</table>

### 802.1X Supplicant Commands

FASTPATH supports 802.1X ("dot1x") supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

4.16.1 dot1x pae

This command sets the port’s dot1x role. The port can serve as either a supplicant or an authenticator.

**Format**

```
dot1x pae {supplicant | authenticator}
```

**Mode**

Interface Config
4.16.2  dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port's attribute needs to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

**Format**

dot1x supplicant port-control{auto | force-authorized | force_unauthorized}

**Mode**

Interface Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.</td>
</tr>
<tr>
<td>force-authorized</td>
<td>Sets the authorization state of the port to Authorized, bypassing the authentication process.</td>
</tr>
<tr>
<td>force-unauthorized</td>
<td>Sets the authorization state of the port to Unauthorized, bypassing the authentication process.</td>
</tr>
</tbody>
</table>

4.16.2.1  no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

**Default**

auto

**Format**

no dot1x supplicant port-control

**Mode**

Interface Config

4.16.3  dot1x supplicant max-start

This command configures the number of attempts that the supplicant makes to find the authenticator before the supplicant assumes that there is no authenticator.

**Default**

3

**Format**

dot1x supplicant max-start <1-10>

**Mode**

Interface Config

4.16.3.1  no dot1x supplicant max-start

This command sets the max-start value to the default.

**Format**

no dot1x supplicant max-start

**Mode**

Interface Config

4.16.4  dot1x supplicant timeout start-period

This command configures the start period timer interval to wait for the EAP identity request from the authenticator.

**Default**

30 seconds

**Format**

dot1x supplicant timeout start-period <1-65535 seconds>

**Mode**

Interface Config
4.16.4.1  no dot1x supplicant timeout start-period
This command sets the start-period value to the default.

Format  no dot1x supplicant timeout start-period
Mode    Interface Config

4.16.5  dot1x supplicant timeout held-period
This command configures the held period timer interval to wait for the next authentication on previous authentication fail.

Default  60 seconds
Format    dot1x supplicant timeout held-period <1-65535 seconds>
Mode      Interface Config

4.16.5.1  no dot1x supplicant timeout held-period
This command sets the held-period value to the default value.

Format  no dot1x supplicant timeout held-period
Mode    Interface Config

4.16.6  dot1x supplicant timeout auth-period
This command configures the authentication period timer interval to wait for the next EAP request challenge from the authenticator.

Default  30 seconds
Format    dot1x supplicant timeout auth-period <1-65535 seconds>
Mode      Interface Config

4.16.6.1  no dot1x supplicant timeout auth-period
This command sets the auth-period value to the default value.

Format  no dot1x supplicant timeout auth-period
Mode    Interface Config

4.16.7  dot1x supplicant user
Use this command to map the given user to the port.

Format  dot1x supplicant user
Mode    Interface Config

4.16.8  show dot1x statistics
This command displays the dot1x port statistics in detail.

Format  show dot1x statistics slot/port
Mode    • Privileged EXEC
        • User EXEC
Example: The following shows example CLI display output for the command.

```
(switch) #show dot1x statistics 0/1
Port........................................... 0/1
EAPOL Frames Received...................... 0
EAPOL Frames Transmitted.................... 0
EAPOL Start Frames Transmitted.............. 3
EAPOL Logoff Frames Received............... 0
EAP Resp/Id frames transmitted............. 0
EAP Response frames transmitted............ 0
EAP Req/Id frames transmitted............... 0
EAP Req frames transmitted.................. 0
Invalid EAPOL frames received.............. 0
EAP length error frames received........... 0
Last EAPOL Frames Version.................. 0
Last EAPOL Frames Source.................... 00:00:00:00:02:01
```

4.17 Storm-Control Commands

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

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

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

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

Use this command to enable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default: disabled

Format: storm-control broadcast

Mode:
- Global Config
- Interface Config

4.17.1.1 no storm-control broadcast

Use this command to disable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format: no storm-control broadcast

Mode:
- Global Config
- Interface Config

4.17.2 storm-control broadcast action

This command configures the broadcast storm recovery action to either shutdown or trap for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to shutdown, the interface that receives the broadcast packets at a rate above the threshold is diagnostically disabled. If set to trap, the interface sends trap messages approximately every 30 seconds until broadcast storm control recovers.

Default: None

Format: storm-control broadcast action {shutdown | trap}

Mode:
- Global Config
- Interface Config

4.17.2.1 no storm-control broadcast action

This command configures the broadcast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format: no storm-control broadcast action

Mode:
- Global Config
- Interface Config

---

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 512 bytes packets are used.
4.17.3 storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) 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 • Global Config
     • Interface Config

4.17.3.1 no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format no storm-control broadcast level
Mode • Global Config
     • Interface Config

4.17.4 storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) 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
     • Interface Config

4.17.4.1 no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format no storm-control broadcast rate
Mode • Global Config
     • Interface Config

4.17.5 storm-control multicast

This command enables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config 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 disabled
Format storm-control multicast
Mode • Global Config
     • Interface Config
4.17.5.1 no storm-control multicast

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

**Format**

```
no storm-control multicast
```

**Mode**

- Global Config
- Interface Config

4.17.6 storm-control multicast action

This command configures the multicast storm recovery action to either `shutdown` or `trap` for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to `shutdown`, the interface that receives multicast packets at a rate above the threshold is diagnostically disabled. The option `trap` sends trap messages approximately every 30 seconds until multicast storm control recovers.

**Default**

None

**Format**

```
storm-control multicast action {shutdown | trap}
```

**Mode**

- Global Config
- Interface Config

4.17.6.1 no storm-control multicast action

This command returns the multicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

**Format**

```
no storm-control multicast action
```

**Mode**

- Global Config
- Interface Config

4.17.7 storm-control multicast level

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) 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**

- Global Config
- Interface Config
4.17.7.1 no storm-control multicast level
This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format: no storm-control multicast level 0-100
Mode:  
• Global Config
• Interface Config

4.17.8 storm-control multicast rate
Use this command to configure the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) 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
• Interface Config

4.17.8.1 no storm-control multicast rate
This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format: no storm-control multicast rate
Mode:  
• Global Config
• Interface Config

4.17.9 storm-control unicast
This command enables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). 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:  
• Global Config
• Interface Config
4.17.9.1 no storm-control unicast
This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

**Format**

```
no storm-control unicast
```

**Mode**
- Global Config
- Interface Config

4.17.10 storm-control unicast action
This command configures the unicast storm recovery action to either *shutdown* or *trap* for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to *shutdown*, the interface that receives unicast packets at a rate above the threshold is diagnostically disabled. The option *trap* sends trap messages approximately every 30 seconds until unicast storm control recovers.

**Default**
None

**Format**

```
storm-control unicast action {shutdown | trap}
```

**Mode**
- Global Config
- Interface Config

4.17.10.1 no storm-control unicast action
This command returns the unicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

**Format**

```
no storm-control unicast action
```

**Mode**
- Global Config
- Interface Config

4.17.11 storm-control unicast level
This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) 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**
- Global Config
- Interface Config
4.17.11.1 **no storm-control unicast level**
This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

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

**Mode**
- Global Config
- Interface Config

4.17.12 **storm-control unicast rate**
Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) 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**
- Global Config
- Interface Config

4.17.12.1 **no storm-control unicast rate**
This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

**Format**
```
no storm-control unicast rate
```

**Mode**
- Global Config
- Interface Config

4.17.13 **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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bcast Mode</td>
<td>Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.</td>
</tr>
<tr>
<td>Bcast Level</td>
<td>The broadcast storm control level.</td>
</tr>
<tr>
<td>Mcast Mode</td>
<td>Shows whether the multicast storm control mode is enabled or disabled.</td>
</tr>
<tr>
<td>Mcast Level</td>
<td>The multicast storm control level.</td>
</tr>
<tr>
<td>Ucast Mode</td>
<td>Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.</td>
</tr>
<tr>
<td>Ucast Level</td>
<td>The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(Routing) #show storm-control

```
Broadcast Storm Control Mode.................. Disable
Broadcast Storm Control Level.................. 5 percent
Broadcast Storm Control Action.................. None
Multicast Storm Control Mode................... Disable
Multicast Storm Control Level.................. 5 percent
Multicast Storm Control Action.................. None
Unicast Storm Control Mode...................... Disable
Unicast Storm Control Level..................... 5 percent
Unicast Storm Control Action.................... None
```

**Example:** The following shows example CLI display output for the command.
(Routing) #show storm-control 1/0/1

```
   Intf  Mode  Level  Action  Mode  Level  Action  Mode  Level  Action
  ------ ------- ------ ------ ------- ------ ------ ------- ------ ------ ------
    1/0/1  Disable 5%  None  Disable 5%  None  Disable 5%  None
```

**Example:** The following shows example CLI display output for the command.
(Routing) #show storm-control all

```
   Intf  Mode  Level  Action  Mode  Level  Action  Mode  Level  Action  Mode  Level  Action
  ------ ------- ------ ------ ------- ------ ------ ------- ------ ------ ------- ------ ------ ------
    1/0/1  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/2  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/3  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/4  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/5  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/6  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/7  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/8  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/9  Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/10 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/11 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/12 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/13 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/14 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/15 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/16 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/17 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/18 Enable 50  Trap  Disable 5%  None  Disable 5%  None
    1/0/19 Enable 50  Trap  Disable 5%  None  Disable 5%  None
```
4.18 Link Dependency Commands
The following commands configure link dependency. Link dependency allows the link status of specified ports to be dependent on the link status of other ports. Consequently, if a port that is depended on by other ports loses link, the dependent ports are administratively disabled or administratively enabled so that the dependent ports links are brought down or up respectively.

4.18.0.1 no link state track
This command clears link-dependency options for the selected group identifier.

Format: no link state track group-id
Mode: Global Config

4.18.1 link state group
Use this command to indicate if the downstream interfaces of the group should mirror or invert the status of the upstream interfaces. The default configuration for a group is down (that is, the downstream interfaces will mirror the upstream link status by going down when all upstream interfaces are down). The action up option causes the downstream interfaces to be up when no upstream interfaces are down.

Default: Down
Format: link state group group-id action {up | down}
Mode: Global Config

4.18.1.1 no link state group
Use this command to restore the link state to down for the group.

Format: no link state group group-id action
Mode: Global Config

4.18.2 link state group downstream
Use this command to add interfaces to the downstream interface list. Adding an interface to a downstream list brings the interface down until an upstream interface is added to the group. The link status then follows the interface specified in the upstream command. To avoid bringing down interfaces, enter the upstream command prior to entering the downstream command.

Format: link state group group-id downstream
Mode: Interface Config
4.18.2.1 no link state group downstream
Use this command to remove the selected interface from the downstream list.

Format: no link state group group-id downstream
Mode: Interface Config

4.18.3 link state group upstream
Use this command to add interfaces to the upstream interface list. Note that an interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same link state group or as a downstream interface in a different link state group, if either configuration creates a circular dependency between groups.

Format: link state group group-id upstream
Mode: Interface Config

4.18.3.1 no link state group upstream
Use this command to remove the selected interfaces from upstream list.

Format: no link state group group-id upstream
Mode: Interface Config

4.18.4 show link state group
Use this command to display information for all configured link-dependency groups or a specified link-dependency group.

Format: show link state group group-id
Mode: Privileged EXEC

Example: This example displays information for all configured link-dependency groups.
(Switching)#show link-state group

<table>
<thead>
<tr>
<th>GroupId</th>
<th>Downstream Interfaces</th>
<th>Upstream Interfaces</th>
<th>Link</th>
<th>Action</th>
<th>Group</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0/3-0/7,0/12-0/17</td>
<td>0/12-0/32,3/5</td>
<td>Link</td>
<td>Up</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0/18,0/27</td>
<td>0/22-0/33,3/1</td>
<td>Link</td>
<td>Up</td>
<td>Down</td>
<td></td>
</tr>
</tbody>
</table>

Example: This example displays information for a specified link-dependency groups
(Switching)#show link state group 1

<table>
<thead>
<tr>
<th>GroupId</th>
<th>Downstream Interfaces</th>
<th>Upstream Interfaces</th>
<th>Link</th>
<th>Action</th>
<th>Group</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0/3-0/7,0/12-0/17</td>
<td>0/12-0/32,3/5</td>
<td>Link</td>
<td>Up</td>
<td>Up</td>
<td></td>
</tr>
</tbody>
</table>

4.18.5 show link state group detail
Use this command to display detailed information about the state of upstream and downstream interfaces for a selected link-dependency group. Group Transitions is a count of the number of times the downstream interface has gone into its “action” state as a result of the upstream interfaces link state.

Format: show link state group group-id detail
Mode: Privileged EXEC
4.19 Link Local Protocol Filtering Commands

Link Local Protocol Filtering (LLPF) allows the switch to filter out multiple proprietary protocol PDUs, such as Port Aggregation Protocol (PAgP), if the problems occur with proprietary protocols running on standards-based switches. If certain protocol PDUs cause unexpected results, LLPF can be enabled to prevent those protocol PDUs from being processed by the switch.

LLPF is supported on the BCM56624, BCM56634, BCM56636, BCM56820, and BCM56334 platforms.

4.19.1 llpf

Use this command to block LLPF protocol(s) on a port.

**Default**

Enabled for the blockudld parameter; disabled for all others.

**Format**

```
llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blockstp | blockall}
```

**Mode**

Interface Config

4.19.1.1 no llpf

Use this command to unblock LLPF protocol(s) on a port.

**Format**

```
no llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blockstp | blockall }
```

**Mode**

Interface Config

4.19.2 show llpf interface

Use this command to display the status of LLPF rules configured on a particular port or on all ports.

**Format**

```
show llpf interface [all | slot/port]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block ISDP</td>
<td>Shows whether the port blocks ISDP PDUs.</td>
</tr>
<tr>
<td>Block VTP</td>
<td>Shows whether the port blocks VTP PDUs.</td>
</tr>
<tr>
<td>Block DTP</td>
<td>Shows whether the port blocks DTP PDUs.</td>
</tr>
<tr>
<td>Block UDLD</td>
<td>Shows whether the port blocks UDLD PDUs.</td>
</tr>
<tr>
<td>Block PAGP</td>
<td>Shows whether the port blocks PAGP PDUs.</td>
</tr>
</tbody>
</table>
4.20 MVR Commands

This section lists the Multicast VLAN Registration (MVR) commands.

4.20.1 mvr

Use this command to enable MVR. This is disabled by default.

| Default   | Disabled                         |
| Format    | mvr                               |
| Mode      | Interface Config; Global Config  |

4.20.1.1 no mvr

Use this command to disable MVR.

| Format    | no mvr                           |
| Mode      | Interface Config; Global Config  |

4.20.2 mvr group

Use this command to add an MVR membership group.

| Format    | mvr group                        |
| Mode      | Global Config                    |

4.20.2.1 no mvr group

Use this command to disable an MVR membership group.

| Format    | no mvr group                     |
| Mode      | Global Config                    |

4.20.3 mvr immediate

Use this command to enable MVR Immediate Leave mode. If the interface is configured as source port, MVR Immediate Leave mode cannot be enabled. MVR Immediate Leave mode disabled by default.

| Default   | Disabled                         |
| Format    | mvr immediate                    |
| Mode      | Interface Config                 |
4.20.3.1 no mvr immediate
Use this command to disable MVR Immediate Leave mode.

Format: \texttt{mvr immediate}
Mode: Interface Config

4.20.4 mvr mode
Use this command to change the MVR mode type. Compatible is the default mode type.

Format: \texttt{mvr mode \text{[compatible | dynamic]}}
Mode: Global Config

4.20.4.1 no mvr mode
Use this command to set the MVR mode type to the default value of compatible.

Format: \texttt{no mvr mode}
Mode: Global Config

4.20.5 mvr querytime
Use this command to set the MVR query response time in units of tenths of a second. The query time is the maximum time to wait for an IGMP membership report on a receiver port before removing the port from the multicast group. The query time only applies to receiver ports and is specified in tenths of a second. The default is 5.

Format: \texttt{mvr querytime \texttt{1-100}}
Mode: Global Config

4.20.5.1 no mvr querytime
Use this command to set the MVR query response time to the default value.

Format: \texttt{no mvr querytime}
Mode: Global Config

4.20.6 mvr type
Use this command to set the MVR port type. The default is none.

Format: \texttt{mvr type \text{[receiver | source]}}
Mode: Interface Config
4.20.6.1 no mvr type
Use this command to reset the MVR port type to None.

Format  no mvr type
Mode     Interface Config

4.20.7 mvr vlan
Use this command to set the MVR multicast VLAN.

Default  1
Format    mvr vlan 1-4093
Mode      Global Config

4.20.7.1 no mvr vlan
Use this command to set the MVR multicast VLAN to the default value.

Format  no mvr vlan
Mode     Global Config

4.20.8 mvr vlan group
Use this command to make a port participate in a specific MVR group. The default value is None.

Format    mvr vlan mvlan group A.B.C.D.
Mode      Interface Config

4.20.8.1 no mvr vlan group
Use this command to remove port participation in the specific MVR group.

Format    no mvr vlan mvlan group A.B.C.D.
Mode      Interface Config

4.20.9 show mvr
Use this command to display global MVR settings.

Format    show mvr
Mode      Privileged EXEC

Example:
(Switching) # show mvr
MVR Disabled.

(Switching) # show mvr
MVR Running.................. TRUE
MVR multicast VLAN........... 1
MVR Max Multicast Groups..... 256
MVR Current multicast groups... 0
MVR Global query response time... 5 (tenths of sec)
MVR Mode...................... compatible
4.20.10  show mvr members
Use this command to display the allocated MVR membership groups.

Format  

Mode  Privileged EXEC

Example:
(Switching) # show mvr members
MVR Disabled

(Switching) # show mvr members

MVR Group IP  Status  Members
-------------  --------  --------------------
224.1.1.1     INACTIVE  0/1, 0/2, 0/3

(Switching) # show mvr members 224.1.1.1

MVR Group IP  Status  Members
-------------  --------  --------------------
224.1.1.1     INACTIVE  0/1, 0/2, 0/3

4.20.11  show mvr interface
Use this command to display the configuration of MVR-enabled interfaces.

Format  show mvr interface [interface-id [members [vlan vlan-id]]]

Mode  Privileged EXEC

Example:
(Switching) # show mvr interface
Port Type  Status          Immediate Leave
------- --------  ------------  ------------------------
0/9  RECEIVER  ACTIVE/inVLAN  DISABLED

(Switching) # show mvr interface 0/4
Type: NONE  Status: INACTIVE/InVLAN  Immediate Leave: DISABLED

show mvr interface 0/23 members
235.0.0.1 STATIC  ACTIVE

(Switching) # show mvr interface 0/23 members vlan 12
235.0.0.1 STATIC  ACTIVE
235.1.1.1 STATIC  ACTIVE

4.20.12  show mvr traffic
Use this command to display global MVR statistics.

Format  show mvr traffic

Mode  Privileged EXEC
Example:
(Switching) # show mvr traffic
IGMP Query Received.................... 0
IGMP Report V1 Received.............. 0
IGMP Report V2 Received.............. 0
IGMP Leave Received................... 0
IGMP Query Transmitted............... 0
IGMP Report V1 Transmitted.......... 0
IGMP Report V2 Transmitted.......... 0
IGMP Leave Transmitted............... 0
IGMP Packet Receive Failures....... 0
IGMP Packet Transmit Failures....... 0

4.20.13 debug mvr trace
Use this command to enable MVR debug tracing. The default value is disabled.

Format debug mvr trace
Mode Privileged EXEC

4.20.13.1 no debug mvr trace
Use this command to disable MVR debug tracing.

Format no debug mvr trace
Mode Privileged EXEC

4.20.14 debug mvr packet
Use this command to enable MVR receive/transmit packets debug tracing. If it is executed without specifying the arguments, both receive and transmit packets debugging is enabled. The default is enabled.

Format debug mvr packet [receive | transmit]
Mode Privileged EXEC

4.20.14.1 no debug mvr packet
Use this command to disable MVR receive/transmit packet debug tracing.

Format no debug mvr packet [receive | transmit]
Mode Privileged EXEC

4.21 Port-Channel/LAG (802.3ad) Commands
This section describes the commands you use to configure port-channels, which is defined in the 802.3ad specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.
4.21.1 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. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

4.21.2 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. You can add a range of ports by specifying the port range when you enter Interface Config mode (for example: interface 0/1-0/4). Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

4.21.3 deleteport (Interface Config)

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical slot/port number of a configured port-channel (or range of port-channels). Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

4.21.4 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. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.
4.21.5  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.
This command can be used to configure a single interface or a range of interfaces.

Default 0x8000
Format lACP admin key key
Mode Interface Config

This command is applicable only to port-channel interfaces.

4.21.5.1 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

4.21.6  lACP collector max-delay
Use this command to configure the port-channel collector max delay. This command can be used to configure a single interface or a range of interfaces. The valid range of delay is 0-65535.

Default 0x8000
Format lACP collector max delay delay
Mode Interface Config

This command is applicable only to port-channel interfaces.

4.21.6.1 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

4.21.7  lACP actor admin key
Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. 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

This command is applicable only to physical interfaces.
4.21.7.1  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

4.21.8    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

This command is applicable only to physical interfaces.

4.21.8.1  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

4.21.9    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

This command is applicable only to physical interfaces.

4.21.9.1  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

This command is applicable only to physical interfaces.
4.21.10  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

This command is applicable only to physical interfaces.

4.21.10.1 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

4.21.11  lACP actor admin state
Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. This command can be used to configure a single interface or a range of interfaces.

Default 0x07
Format  lACP actor admin state {individual|longtimeout|passive}
Mode    Interface Config

This command is applicable only to physical interfaces.

4.21.11.1 no lACP actor admin state
Use this command to configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

Both the no portlacptimeout and the no lACP actor admin state commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in show running-config.

Format  no lACP actor admin state {individual|longtimeout|passive}
Mode    Interface Config

4.21.12  lACP actor port priority
Use this command to configure the priority value assigned to the Aggregation Port for an interface or range of interfaces. The valid range for priority is 0 to 65535.

Default 0x80
Format  lACP actor port priority 0-65535
Mode    Interface Config
4.21.12.1 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

4.21.13 lacp partner admin key
Use this command to configure the administrative value of the Key for the protocol partner. This command can be used to configure a single interface or a range of interfaces. The valid range for key is 0 to 65535.

Default  0x0
Format    lacp partner admin key key
Mode      Interface Config

4.21.13.1 no lacp partner admin key
Use this command to set the administrative value of the Key for the protocol partner to the default.

Format  no lacp partner admin key
Mode    Interface Config

4.21.14 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

This command is applicable only to physical interfaces.
4.21.14.1  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

4.21.15  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

This command is applicable only to physical interfaces.

4.21.15.1  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

This command is applicable only to physical interfaces.

4.21.16  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

This command is applicable only to physical interfaces.

4.21.16.1  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

4.21.17  lacp partner port id
Use this command to configure the LACP partner port id. This command can be used to configure a single interface or a range of interfaces. The valid range for port-id is 0 to 65535.
4.21.17.1  no lacp partner port id
Use this command to set the LACP partner port id to the default.

Format  no lacp partner port-id
Mode    Interface Config

Notice: This command is applicable only to physical interfaces.

4.21.18  lacp partner port priority
Use this command to configure the LACP partner port priority. This command can be used to configure a single interface or a range of interfaces. The valid range for priority is 0 to 65535.

Default  0x0
Format    lacp partner port priority priority
Mode      Interface Config

Notice: This command is applicable only to physical interfaces.

4.21.18.1  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

4.21.19  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. This command can be used to configure a single interface or a range of interfaces. 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

Notice: This command is applicable only to physical interfaces.
4.21.19 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

4.21.20 lacp partner system priority
Use this command to configure the administrative value of the priority associated with the Partner’s System ID. This command can be used to configure a single interface or a range of interfaces. The valid range for priority is 0 to 65535.

Default 0x0
Format lacp partner system priority 0-65535
Mode Interface Config

---

This command is applicable only to physical interfaces.

4.21.20.1 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

4.21.21 interface lag
Use this command to enter Interface configuration mode for the specified LAG.

Format interface lag lag-interface-number
Mode Global Config

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

Default enabled
Format port-channel static
Mode Interface Config
4.21.22.1 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

4.21.23 port lacpmode
This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

**Default**
enabled

**Format**
port lacpmode

**Mode**
Interface Config

4.21.23.1 no port lacpmode
This command disables Link Aggregation Control Protocol (LACP) on a port.

**Format**
no port lacpmode

**Mode**
Interface Config

4.21.24 port lacpmode enable all
This command enables Link Aggregation Control Protocol (LACP) on all ports.

**Format**
port lacpmode enable all

**Mode**
Global Config

4.21.24.1 no port lacpmode enable all
This command disables Link Aggregation Control Protocol (LACP) on all ports.

**Format**
no port lacpmode enable all

**Mode**
Global Config

4.21.25 port lacptimeout (Interface Config)
This command sets the timeout on a physical interface or range of 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**
Interface Config
4.21.25.1 **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

---

**NOTICE**
Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

4.21.26 **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

4.21.26.1 **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

---

**NOTICE**
Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

4.21.27 **port-channel adminmode**
This command enables all configured port-channels with the same administrative mode setting.

**Format**
```
port-channel adminmode all
```

**Mode**
Global Config

4.21.27.1 **no port-channel adminmode**
This command disables all configured port-channels with the same administrative mode setting.

**Format**
```
no port-channel adminmode all
```

**Mode**
Global Config
4.21.28  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. Instead of slot/port, lag lag-intf-num can also be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Default enabled  
Format port-channel linktrap {Logical slot/port | all}  
Mode Global Config

4.21.28.1  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

4.21.29  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.

This command can be configured for a single interface, a range of interfaces, or all interfaces. Instead of slot/port, lag lag-intf-num can also be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Default 3  
Format port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7} {slot/port | all}  
Mode Interface Config  
Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Source MAC, VLAN, EtherType, and incoming port associated with the packet</td>
</tr>
<tr>
<td>2</td>
<td>Destination MAC, VLAN, EtherType, and incoming port associated with the packet</td>
</tr>
<tr>
<td>3</td>
<td>Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet</td>
</tr>
<tr>
<td>4</td>
<td>Source IP and Source TCP/UDP fields of the packet</td>
</tr>
<tr>
<td>5</td>
<td>Destination IP and Destination TCP/UDP Port fields of the packet</td>
</tr>
<tr>
<td>6</td>
<td>Source/Destination IP and source/destination TCP/UDP Port fields of the packet</td>
</tr>
<tr>
<td>7</td>
<td>Enhanced hashing mode</td>
</tr>
<tr>
<td>slot/port</td>
<td>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.</td>
</tr>
</tbody>
</table>
4.21.29.1 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>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.</td>
</tr>
<tr>
<td>all</td>
<td></td>
</tr>
</tbody>
</table>

4.21.30 port-channel local-preference

This command enables the local-preference mode on a port-channel (LAG) interface or range of interfaces. By default, the local-preference mode for a port-channel is disabled. This command can be used only on port-channel interfaces.

**Default**

disable

**Format**

port-channel local-preference

**Mode**

Interface Config

4.21.30.1 no port-channel local-preference

This command disables the local-preference mode on a port-channel.

**Format**

no port-channel local-preference

**Mode**

Interface Config

4.21.31 port-channel min-links

This command configures the port-channel's minimum links for lag interfaces.

**Default**

1

**Format**

port-channel min-links 1-8

**Mode**

Interface Config

4.21.32 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. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

**Format**

port-channel name {Logical slot/port} name

**Mode**

Global Config
4.21.33  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

4.21.33.1 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

4.21.34  show hashdest

Use this command to predict how packets are forwarded over a LAG or to the next hop device when ECMP is the destination. Given the link aggregation method, ingress physical port and values of various packet fields, this command predicts an egress physical port within the LAG or ECMP for the packet.

Format     show hashdest {lag lag-id | ecmp prefix/prefix-length} in_port unit/slot/port src-mac macaddr dst-mac macaddr [vlan vlan-id] ethertype 0xXXXX [src-ip {ipv4-addr | ipv6-addr} dst-ip {ipv4-addr | ipv6-addr} protocol pid src-l4-port port-num dst-l4-port port-num]

Mode       Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag</td>
<td>The LAG group for which to display the egress physical port.</td>
</tr>
<tr>
<td>ecmp</td>
<td>The IP address of the ECMP group for which to display the egress physical port.</td>
</tr>
<tr>
<td>in_port</td>
<td>The incoming physical port for the system.</td>
</tr>
<tr>
<td>src-mac</td>
<td>The source MAC address.</td>
</tr>
<tr>
<td>dst-mac</td>
<td>The destination MAC address.</td>
</tr>
<tr>
<td>vlan</td>
<td>The VLAN ID for VLAN-tagged packets. Do not use this parameter or enter 0 for non-VLAN-tagged packets.</td>
</tr>
<tr>
<td>ethertype</td>
<td>The 16-bit EtherType value, in the form 0xXXXX. For layer 3 packets, hash prediction is only available for IPv4 (0x0800) and and IPv6 (0x86DD).</td>
</tr>
<tr>
<td>src-ip</td>
<td>The source IP address, entered as x.x.x.x for IPv4 or x:x:x:x:x:x:x:x for IPv6 packets.</td>
</tr>
<tr>
<td>dst-ip</td>
<td>The destination IP address, entered as x.x.x.x for IPv4 or x:x:x:x:x:x:x:x for IPv6 packets.</td>
</tr>
<tr>
<td>protocol</td>
<td>The protocol ID.</td>
</tr>
<tr>
<td>src-l4-port</td>
<td>The layer 4 source port.</td>
</tr>
<tr>
<td>dst-l4-port</td>
<td>The layer 4 destination port.</td>
</tr>
</tbody>
</table>

Example: Layer 2 VLAN tagged packet forwarded to a LAG

(Routing) #show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E vlan 10 ethertype 0x8870

<table>
<thead>
<tr>
<th>LAG</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0/29</td>
</tr>
</tbody>
</table>
Example: Layer 2 non-VLAN tagged packet forwarded to a LAG
(Routing) # show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E
ethertype 0x8870

LAG              Destination Port
----------------- ------------------------
1                0/31

Example: Non-VLAN tagged IPv4 UDP packet forwarded to a LAG
(Routing) # show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E
ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 17 src-l4-port 63 dst-l4-port 64

LAG              Destination Port
----------------- ------------------------
1                0/32

Example: VLAN tagged IPv4 TCP packet forwarded to a LAG
(Routing) # show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E
ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 6 src-l4-port 67 dst-l4-port 68

LAG              Destination Port
----------------- ------------------------
1                0/31

Example: Non-VLAN tagged IPv4 UDP packet forwarded to an ECMP group
(Routing) # show hashdest ecmp 10.0.0.2/16 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E vlan 0 ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 17 src-l4-port 63
dst-l4-port 64

Egress Port
----------------
30.0.0.2 on interface 0/31

Example: VLAN tagged IPv4 TCP packet forwarded to an ECMP group
(Routing) # show hashdest ecmp 10.0.0.2/16 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E vlan 10 ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 6 src-l4-port 67
dst-l4-port 68

Egress Port
----------------
6.0.0.2 on interface 0/31

Example: Non-VLAN tagged IPv6 UDP packet forwarded to an ECMP group
(Routing) # show hashdest ecmp 4001::200/64 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E ethertype 0x86dd src-ip 7001:0:0:0:0:0:0:2 dst-ip 3001:0:0:0:0:0:0:2 protocol 17
src-l4-port 63 dst-l4-port 64

Egress Port
----------------
6001::200 on interface 0/31

Example: Non-VLAN tagged IPv6 TCP packet forwarded to an ECMP group
(Routing) # show hashdest ecmp 6001::200/64 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E ethertype 0x86dd src-ip 7001:0:0:0:0:0:0:2 dst-ip 3001:0:0:0:0:0:0:2 protocol 6
src-l4-port 67 dst-l4-port 68

Egress Port
----------------
8001::200 on interface 0/32
4.21.35  show lacp actor

Use this command to display LACP actor attributes. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Format  show lacp actor {slot/port|all}
Mode    Global Config

The following output parameters are displayed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Priority</td>
<td>The administrative value of the Key.</td>
</tr>
<tr>
<td>Actor Admin Key</td>
<td>The administrative value of the Key.</td>
</tr>
<tr>
<td>Port Priority</td>
<td>The priority value assigned to the Aggregation Port.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative values of the actor state as transmitted by the Actor in LACPDUs.</td>
</tr>
</tbody>
</table>

4.21.36  show lacp partner

Use this command to display LACP partner attributes. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Format  show lacp partner {slot/port|all}
Mode    Privileged EXEC

The following output parameters are displayed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Priority</td>
<td>The administrative value of priority associated with the Partner's System ID.</td>
</tr>
<tr>
<td>System-ID</td>
<td>Represents the administrative value of the Aggregation Port's protocol Partner's System ID.</td>
</tr>
<tr>
<td>Admin Key</td>
<td>The administrative value of the Key for the protocol Partner.</td>
</tr>
<tr>
<td>Port Priority</td>
<td>The administrative value of the Key for protocol Partner.</td>
</tr>
<tr>
<td>Port-ID</td>
<td>The administrative value of the port number for the protocol Partner.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative values of the actor state for the protocol Partner.</td>
</tr>
</tbody>
</table>

4.21.37  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. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Format  show port-channel brief
Mode    •  User EXEC

For each port-channel the following information is displayed:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Interface</td>
<td>The slot/port of the logical interface.</td>
</tr>
<tr>
<td>Port-channel Name</td>
<td>The name of port-channel (LAG) interface.</td>
</tr>
<tr>
<td>Link-State</td>
<td>Shows whether the link is up or down.</td>
</tr>
</tbody>
</table>
4.21.38  show port-channel

This command displays an overview of all port-channels (LAGs) on the switch. Instead of slot/port, lag Intf-num can be used as an alternate way to specify the LAG interface. lag Intf-num can also be used to specify the LAG interface where lag Intf-num is the LAG port number.

Format  show port-channel

Mode  

• Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Flag</td>
<td>Shows whether trap flags are enabled or disabled.</td>
</tr>
<tr>
<td>Type</td>
<td>Shows whether the port-channel is statically or dynamically maintained.</td>
</tr>
<tr>
<td>Mbr Ports</td>
<td>The members of this port-channel.</td>
</tr>
<tr>
<td>Active Ports</td>
<td>The ports that are actively participating in the port-channel.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Interface</td>
<td>The valid slot/port number.</td>
</tr>
<tr>
<td>Port-Channel Name</td>
<td>The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.</td>
</tr>
<tr>
<td>Link State</td>
<td>Indicates whether the Link is up or down.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>May be enabled or disabled. The factory default is enabled.</td>
</tr>
<tr>
<td>Type</td>
<td>The status designating whether a particular port-channel (LAG) is statically or dynamically maintained.</td>
</tr>
<tr>
<td></td>
<td>• Static - The port-channel is statically maintained.</td>
</tr>
<tr>
<td></td>
<td>• Dynamic - The port-channel is dynamically maintained.</td>
</tr>
<tr>
<td>Load Balance Option</td>
<td>The load balance option associated with this LAG. See “port-channel load-balance” on page 400.</td>
</tr>
<tr>
<td>Local Preference Mode</td>
<td>Indicates whether the local preference mode is enabled or disabled.</td>
</tr>
<tr>
<td>Mbr Ports</td>
<td>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).</td>
</tr>
<tr>
<td>Device Timeout</td>
<td>For each port, lists the timeout (long or short) for Device Type (actor or partner).</td>
</tr>
<tr>
<td>Port Speed</td>
<td>Speed of the port-channel port.</td>
</tr>
<tr>
<td>Active Ports</td>
<td>This field lists ports that are actively participating in the port-channel (LAG).</td>
</tr>
</tbody>
</table>

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

(Switch) #show port-channel 3/1

```
Local Interface................................. 3/1
Channel Name..................................... ch1
Link State....................................... Up
Admin Mode...................................... Enabled
Type............................................... Static
Load Balance Option............................ 3
(Src/Dest MAC, VLAN, EType, incoming port)
Local Preference Mode.......................... Enabled

Mbr  Device/ Port  Port  Port
     Timeout  Speed  Active
--------- --------- ---------
0/1  actor/long  Auto  True
     partner/long
0/2  actor/long  Auto  True
```
4.21.39  show port-channel system priority

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

Format  show port-channel system priority
Mode    Privileged EXEC

4.21.40  show port-channel counters

Use this command to display port-channel counters for the specified port.

Format  show port-channel slot/port counters
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Interface</td>
<td>The valid slot/port number.</td>
</tr>
<tr>
<td>Channel Name</td>
<td>The name of this port-channel (LAG).</td>
</tr>
<tr>
<td>Link State</td>
<td>Indicates whether the Link is up or down.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>May be enabled or disabled. The factory default is enabled.</td>
</tr>
<tr>
<td>Port Channel Flap Count</td>
<td>The number of times the port-channel was inactive.</td>
</tr>
<tr>
<td>Mbr Ports</td>
<td>The slot/port for the port member.</td>
</tr>
<tr>
<td>Mbr Flap Counters</td>
<td>The number of times a port member is inactive, either because the link is down, or the admin state is disabled.</td>
</tr>
</tbody>
</table>

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

(Switch) #show port-channel 3/1 counters

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>3/1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Name</td>
<td>ch1</td>
</tr>
<tr>
<td>Link State</td>
<td>Down</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>Port Channel Flap Count</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mbr Flap Counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1 0</td>
</tr>
<tr>
<td>0/2 0</td>
</tr>
<tr>
<td>0/3 1</td>
</tr>
<tr>
<td>0/4 0</td>
</tr>
<tr>
<td>0/5 0</td>
</tr>
<tr>
<td>0/6 0</td>
</tr>
<tr>
<td>0/7 0</td>
</tr>
<tr>
<td>0/8 0</td>
</tr>
</tbody>
</table>
4.21.41 clear port-channel counters
Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

**Format**
clear port-channel {lag-intf-num | slot/port} counters

**Mode**
Privileged EXEC

4.21.42 clear port-channel all counters
Use this command to clear and reset all port-channel and member flap counters for the specified interface.

**Format**
clear port-channel all counters

**Mode**
Privileged EXEC

4.21.43 set bpdu forwarding
This command configures BPDU forwarding. The default behavior is that received BPDU is sent to the CPU and handled. The BPDU frame is not forwarded/switched. If this feature is enabled the BPDU frame is not longer sent to CPU but forwarded/switched on all ports.

Note, that you have to save the configuration and reboot the system to activate a new setting.

**Format**
set bpdu forwarding

**Mode**
Privileged EXEC

4.21.43.1 no set bpdu forwarding
This command disabled BPDU forwarding.

Note, that you have to save the configuration and reboot the system to activate a new setting.

**Format**
no set bpdu forwarding

**Mode**
Privileged EXEC

4.21.44 show bpdu forwarding
This command displays the BPDU forwarding setting. The values for the current active setting and the value for the configured setting are indicated.

**Format**
show bpdu forwarding

**Mode**
Privileged EXEC

4.22 VPC Commands
VPC (also known as MLAG) enables a LAG to be created across two independent switches, so that some member ports of a VPC can reside on one switch and the other members of a VPC can reside on another switch. The partner device on the remote side can be a VPC-unaware unit. To the unaware unit, the VPC appears to be a single LAG connected to a single switch.
4.22.1  vpc domain

Use this command to enter into VPC configuration mode and creates a VPC domain with the specified domain-id. Only one VPC domain can be created on a given device. The domain-id of the VPC domain should be equal to the one configured on the other VPC peer with which this device wants to form a VPC pair. The configured VPC domain-ids are exchanged during role election and if they are configured differently on the peer devices, the VPC does not become operational.

The administrator needs to ensure that the no two VPC domains can share the same VPC domain-id. Domain-id is used to derive the auto-generated VPC MAC address that is used in the actor ID field in the LACP PDUs and STP BPDUs sent out on VPC interfaces. When two VPC domains have the same domain-id, it leads to the same actor IDs and results in LACP convergence issues and STP convergence issues.

The range of domain id is 1-255.

Format  vpc domain domain-id
Mode     Global Config

4.22.1.1  no vpc domain

Use this command to deletes the VPC domain, disable peer-keepalive, disable peer-detection, and reset the configured parameters (role priority, VPC MAC address and VPC system priority) for the VPC domain.

Format  no vpc domain domain-id
Mode     Global Config

4.22.2  feature vpc

This command enables VPC globally. VPC role election occurs if both VPC and the keepalive state machine are enabled (see "peer-keepalive timeout" on page 410). Peer link also has to be configured for role election to occur.

Format  feature vpc
Mode     Global Config

4.22.2.1  no feature vpc

This command disables VPC.

Format  no feature vpc
Mode     Global Config

4.22.3  peer detection enable

This command starts the dual control plane detection protocol (DCPDP) on the VPC switch. The peer VPC switch’s IP address must be configured for the DCPDP to start on an VPC switch.

Default  None
Format    peer detection enable
Mode      VPC Config

4.22.3.1  no peer detection enable

This command disables the dual control plane (DCPDP) detection protocol on the VPC switch.

Format  no peer detection enable
Mode     VPC Config
4.22.4 peer detection interval
Use this command to configure the DCPDP transmission interval and reception timeout.
The configurable transmission interval range is 200 ms–4000 ms. The configurable reception timeout range is 700 ms–14000 ms. The default transmission interval is 1000 ms; the default reception timeout is 3500 ms.

Default
• Transmission interval: 1000 ms
• Reception timeout: 3500 ms

Format peer detection interval msecs timeout seconds
Mode VPC Config

4.22.4.1 no peer detection interval
Use this command to reset the DCPDP transmission interval and reception timeout to default values.

Format no peer detection interval msecs timeout seconds
Mode VPC Config

4.22.5 peer-keepalive destination
This command configures the IP address of the peer VPC switch, which is the destination IP address of the dual control plane detection protocol (DCPDP) on the peer VPC switch. This configuration is used by the dual control plane detection protocol (DCPDP) on the VPC switches. It also configures the source IP address of the DCPDP message, which is the self IP on the VPC switch. The UDP port on which the VPC switch listens to the DCPDP messages can also be configured with this command.
The configurable range for the UDP port 1 to 65535 (Default is 60000).

Format peer-keepalive destination ipaddress switch ipaddress [udp-port port]
Mode VPC Config

4.22.5.1 no peer-keepalive destination
This command unconfigures the self IP address, peer IP address, and the UDP port.

Format no peer-keepalive destination ipaddress switch ipaddress [udp-port port]
Mode VPC Config

4.22.6 peer-keepalive enable
This command starts the keepalive state machine on the VPC device, if VPC is globally enabled.

Default Disabled

Format peer-keepalive enable
Mode VPC Config

4.22.6.1 no peer-keepalive enable
This command stops the keepalive state machine of the VPC switch.

Format no peer-keepalive enable
Mode VPC Config
4.22.7 peer-keepalive timeout

This command configures the peer keepalive timeout value (in seconds). If an VPC switch does not receive a keepalive message from the peer for the duration of this timeout value, it transitions its role (if required).

The configurable range is 2 to 15 seconds. The default is 5 seconds.

Format peer-keepalive timeout value
Mode VPC Config

4.22.7.1 no peer-keepalive timeout

This command resets the keepalive timeout to the default value of 5 seconds.

Format no keepalive timeout
Mode VPC Config

4.22.8 role priority

This command configures VPC switch priority. This value is used for VPC role election. The priority value is sent to the peer in the VPC keepalive messages. The VPC switch with lower priority becomes the Primary and the switch with higher priority becomes the Secondary. If both VPC peer switches have the same role priority, the device with the lower system MAC address becomes the Primary.

The priority can be between 1 and 255 seconds. The default is 100.

Format role priority value
Mode VPC Config

4.22.8.1 no role priority

This command resets the keepalive priority and timeout to the default value of 100.

Format no role priority
Mode VPC Config

4.22.9 system-mac

Use this command to manually configure the MAC address for the VPC domain. The VPC MAC address should be configured same on both the peer devices. The specified MAC address should be a unicast MAC address in <aa:bb:cc:dd:ee:ff> format and cannot be equal to the MAC address of either the primary VPC or secondary VPC device. The configured VPC MAC address is exchanged during role election and, if they are configured differently on the peer devices, VPC does not become operational.

The mac-address is used in the LACP PDUs and STP BPDUs that are sent out on VPC member ports, if VPC primary device election takes place after the VPC MAC address is configured. When the VPC MAC address is configured after the VPC primary device is elected, the operational VPC MAC address is used in the LACP PDUs and STP BPDUs instead of the configured VPC MAC address.
4.22.9.1 no system-mac
This command unconfigures the manually configured VPC MAC address for the VPC domain.

Format: no system-mac
Mode: VPC Domain

4.22.10 system-priority
Use this command to manually configure a system priority for the VPC domain. The system-priority should be configured identically on both VPC peers. If the configured VPC system priority is different on VPC peers, the VPC will not come up.

The system-priority is used in the LACP PDUs that are sent out on VPC member ports if VPC primary device election takes place after the VPC system priorities are configured. When the VPC system priority is configured after the VPC primary device is elected, the operational VPC system priority is used in the LACP PDUs instead of the configured VPC system priority.

The configurable range is 1 to 65535. The default is 32767.

Format: system-priority priority
Mode: VPC Domain

4.22.10.1 no system-priority
This command restores the VPC system priority to the default value.

Format: no system-priority priority
Mode: VPC Domain

4.22.11 vpc
This command configures a port-channel (LAG) as part of an VPC. Upon issuing this command, the port-channel is down until the port-channel member information is exchanged and agreed between the VPC peer switches.

The configurable range for the VPC id 1 to (Max number of LAG interfaces (64) -1)

Default: none
Format: vpc id
Mode: LAG Interface

4.22.11.1 no vpc
This command unconfigures a port-channel as VPC.

Format: no vpc id
Mode: LAG Interface
4.22.12  vpc peer-link
This command configures a port channel as the VPC peer link.

Format  vpc peer-link
Mode    LAG Interface

4.22.12.1  no vpc peer-link
This command unconfigures a port channel as the VPC peer link.

Format  no vpc peer-link
Mode    LAG Interface

4.22.13  show running-config vpc
Use this command to display running configuration information for virtual port channels (VPC).

Format  show running-config vpc
Mode    Privileged EXEC

Example:
(Switching) # show running-config vpc

feature vpc
vpc domain 1
role priority 120
system-mac 00:10:18:82:1A:A0
system-priority 32767
peer-keepalive destination 1.1.1.1 source 1.1.1.2
        peer detection interval 2000  timeout 6000

interface lag 1
    vpc peer-link

interface lag 2
    vpc 2

4.22.14  show vpc
This command displays information about an VPC. The configuration and operational modes of the VPC are displayed; the VPC is operationally enabled if all the preconditions are met. The port-channel that is configured as an VPC interface is also displayed with the member ports on the current switch and peer switch (with their link status)

Format  show vpc id
Mode    User EXEC

Example: The following shows an example of the command.
(Switching) # show vpc 10
VPC id#10
-------------------
Config mode............................Enabled
Operational mode.....................Enabled
Port channel........................3/1
Self member ports Status
------------------- -------
  0/2 UP
  0/6 DOWN
Peer member ports Status
----------------------------------------
0/8 UP

4.22.15 show vpc brief

This command displays the VPC global status and current VPC operational mode (the VPC is in operational mode if the preconditions are met). The peerlink and keepalive statuses as well as the number of configured and operational VPCs and the system MAC and role are displayed.

Format show vpc brief
Mode Privileged EXEC

Example: The following shows an example of the command.

(Switching) # show vpc brief
VPC Domain ID..........................1
VPC config Mode......................... Enabled
Keepalive config mode................. Enabled
VPC operational Mode.................. Enabled
Self Role................................ Primary
Peer Role............................... Secondary
Peer detection......................... Disabled
Operational VPC MAC.................... aa:bb:cc:dd:ee:ff
Operational VPC system priority.........32767

Peer-link details
------------------
Interface......................... 3/2
Peer link status................... UP
Peer-link STP Mode.................. Disabled
Configured Vlans.................... 1
Egress tagging...................... none

VPC Details
----------
Number of VPCs configured............. 1
Number of VPCs operational........... 1

VPC id# 1
--------
Interface................................ 3/1
Configured Vlans.................... 1
VPC Interface State.................. Active

<table>
<thead>
<tr>
<th>Local MemberPorts</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/19</td>
<td>UP</td>
</tr>
<tr>
<td>0/20</td>
<td>UP</td>
</tr>
<tr>
<td>0/21</td>
<td>UP</td>
</tr>
<tr>
<td>0/22</td>
<td>UP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peer MemberPorts</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/27</td>
<td>UP</td>
</tr>
<tr>
<td>0/28</td>
<td>UP</td>
</tr>
<tr>
<td>0/29</td>
<td>UP</td>
</tr>
<tr>
<td>0/30</td>
<td>UP</td>
</tr>
</tbody>
</table>
4.22.16  show vpc consistency-parameters

Use this command to display global consistency parameters and LAG interface consistency parameters for virtual port channels (VPC) on the switch.

**Format**  
show vpc consistency-parameters {global | interface lag lag-id}

**Mode**  
Privileged EXEC

**Example:**

```
switch# show vpc consistency-parameters global
Name        Value
--------------- ------------------------------
STP Mode    Enabled
STP Version EEE 802.1s
BPDU Filter Mode Enabled
BPDU Guard Mode Enabled
MST Instances 1,2,4
FDB Aging Time 300 seconds
VPC system MAC address <AA:BB:CC:DD:EE:FF>
VPC system priority 32767
VPC Domain ID 1
MST VLAN Configuration
Instance    Associated VLANS
----------- --------------------------
7,8,10,20    4,5,40-50
2            30,32,34-38

switch# show vpc consistency-parameters interface lag 2
Name        Value
--------------- ------------------------------
Port Channel Mode Enabled
STP Mode    Enabled
BPDU Filter Mode Enabled
BPDU Flood Mode Enabled
Auto-edge   FALSE
TCN Guard   True
Port Cost   2
Edge Port   True
Root Guard  True
Loop Guard  True
Hash Mode   3
Minimum Links 1
Channel Type Static
Configured VLANs 4,5,7,8
MTU         1518

Active Port Speed Duplex
---------- --------- ---------
  0/1  100      Full
  0/2  100      Full

MST VLAN Configuration

Instance    Associated VLANS
----------- --------------------------
  1            7,8
```
2, 4,5
PV(R)STP Configuration:
STP port-priority <0-240>

VLAN port-priority cost
-------- --------------- ---------------
<ID> <0-240> auto | <1-20000000>

4.22.17 show vpc peer-keepalive
This command displays the peer VPC switch IP address used by the dual control plane detection protocol. The port used for the DCPDP is shown. This command also displays if peer detection is enabled. If enabled, the detection status is displayed. The DCPDP message transmission interval and reception timeout are also displayed.

**Format**
show vpc peer-keepalive

**Mode**
User EXEC

**Example:** The following shows an example of the command.
(Switching) # show vpc peer-keepalive
Peer IP address.......................... 10.130.14.55
Source IP address......................... 10.130.14.54
UDP port................................ 50000
Peer detection admin status............. Enabled
Peer detection operational status....... Down
Peer is detected........................ True
Configured Tx interval................... 1000 milliseconds
Configured Rx timeout................... 3500 milliseconds
Operational Tx interval............... 500 milliseconds
Operational Rx timeout............... 2000 milliseconds

4.22.18 show vpc role
This command displays information about the keepalive status and parameters. The role of the VPC switch as well as the system MAC address and priority are displayed.

**Format**
show vpc role

**Mode**
User EXEC

**Example:** The following shows an example of the command.
(Switching) # show vpc role
Self
---
VPC domain ID..........................1
Keepalive config mode................. Enabled
Keepalive operational mode............ Enabled
Role Priority..........................100
Configured VPC MAC....................<AA:BB:CC:DD:EE:FF>
Operational VPC MAC...................<AA:BB:CC:DD:EE:FF>
Configured VPC system priority.......32767
Operational VPC system priority.......32767
Local System MAC.......................00:10:18:82:18:63
Timeout.................................. 5
VPC State................................ Primary
VPC Role................................ Primary

Peer
---
VPC Domain ID..........................1
Role Priority..........................100
4.22.19 show vpc statistics

This command displays counters for the keepalive messages transmitted and received by the VPC switch.

**Format**

```
show vpc statistics {peer-keepalive | peer-link}
```

**Mode**

User EXEC

**Example:** The following shows examples of the command.

**Example 1**

(Switching) # show vpc statistics peer-keepalive
Total transmitted....................... 123
Tx successful.............................. 118
Tx errors...................................... 5
Total received............................ 115
Rx successful............................... 108
Rx Errors.................................... 7
Timeout counter.......................... 6

**Example 2:**

(Switching) # show vpc statistics peer-link
Peer link control messages transmitted........... 123
Peer link control messages Rx errors............... 5
Peer link control messages Rx timeout............ 4
Peer link control messages ACK transmitted...... 34
Peer link control messages ACK Rx errors........ 5
Peer link control messages received............... 115
Peer link data messages transmitted.............. 123
Peer link data messages Rx errors................. 5
Peer link data messages Rx timeout............... 4
Peer link data messages ACK Rx errors........... 34
Peer link data messages received................ 115
Peer link BPDU’s transmitted to peer............ 123
Peer link BPDU’s Rx error..................... 9
Peer link BPDU’s received from peer............. 143
Peer link BPDU’s Rx error..................... 1
Peer link LACPDU’s transmitted to peer.......... 123
Peer link LACPDU’s Rx error................... 9
Peer link LACPDU’s received from peer........... 143
4.22.20  clear vpc statistics
This command clears all the keepalive statistics.

Format     clear vpc statistics {peer-keepalive | peer-link}
Mode       User EXEC

Example: The following shows an example of the command.
(Switching) # clear vpc statistics peer-keepalive
(Switching) # clear vpc statistics peer-link

4.22.21  debug vpc peer-keepalive
This command enables debug traces of the keepalive state machine transitions.

Format     debug vpc peer-keepalive
Mode       User EXEC

4.22.22  debug vpc peer-link data-message
This command enables debug traces for the control messages exchanged between the VPC devices on the peer link.

Format     debug vpc peer-link data-message
Mode       User EXEC

4.22.23  debug vpc peer-link control-message async
This command enables debug traces for the asynchronous reliable control messages exchanged between the MLAG devices on the peer link. For error, only the errors in the communication are traced. For msg, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format     debug vpc peer-link control-message async {error | msg [receive | transmit]}
Mode       User EXEC

4.22.24  debug vpc peer-link control-message bulk
This command enables debug traces for the periodic control messages exchanged between the MLAG devices on the peer link. For error, only the errors in the communication are traced. For msg, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format     debug vpc peer-link control-message bulk {error | msg [receive | transmit]}
Mode       User EXEC

4.22.25  debug vpc peer-link control-message ckpt
This command enables debug traces for the checkpointing control messages exchanged between the MLAG devices on the peer link. For error, only the errors in the communication are traced. For msg, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format     debug vpc peer-link control-message ckpt {error | msg [receive | transmit]}
Mode       User EXEC
4.22.26 debug vpc peer detection

This command enables debug traces for the dual control plane detection protocol. Traces are seen when the DCPDP transmits or receives detection packets to or from the peer VPC switch.

**Format**
```
display vpc peer detection
```

**Mode**
User EXEC

4.23 Port Mirroring Commands

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.

4.23.1 monitor session source

This command configures the source interface for a selected monitor session. Use the `source interface unit/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.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

---

**NOTICE**

The source and destination cannot be configured as remote on the same device.

The commands described below add a mirrored port (source port) to a session identified with `session-id`. The `session-id` parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is `L7_MIRRORING_MAX_SESSIONS`. Option `rx` is used to monitor only ingress packets. Option `tx` is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

---

**NOTICE**

If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

---

**NOTICE**

On the intermediate switch, RSPAN VLAN should be created, the ports connected towards Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on the interface on the intermediate switch connected towards the Destination switch.

**Default**
None

**Format**
```
monitor session session-id source {interface {unit/slot/port | cpu | lag} | vlan vlan-id | remote vlan vlan-id} [{rx | tx}]
```

**Mode**
Global Config
4.23.1 no monitor session source

This command removes the specified mirrored port from the selected port mirroring session.

Default None

Format no monitor session session-id source {interface {unit/slot/port | cpu | lag | vlan | remote vlan}

Mode Global Config

4.23.2 monitor session destination

This command configures the probe interface for a selected monitor session. This command configures a probe port and a monitored port for monitor session (port monitoring). 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.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

**NOTICE**

The source and destination cannot be configured as remote on the same device.

The reflector-port is configured at the source switch along with the destination RSPAN VLAN. The reflector-port forwards the mirrored traffic towards the destination switch.

**NOTICE**

This port must be configured with RSPAN VLAN membership.

Use the destination interface unit/slot/port to specify the interface to receive the monitored traffic.

The commands described below add a mirrored port (source port) to a session identified with session-id. The session-id parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS. Option rx is used to monitor only ingress packets. Option tx is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

**NOTICE**

If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

**NOTICE**

On the intermediate switch, RSPAN VLAN should be created, the ports connected towards Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on the interface on the intermediate switch connected towards the Destination switch.

Default None

Format monitor session session-id destination {interface unit/slot/port | remote vlan vlan-id reflector-port unit/slot/port}

Mode Global Config
4.23.2.1 no monitor session destination
This command removes the specified probe port from the selected port mirroring session.

**Format**

```
no monitor session session-id destination {interface unit/slot/port | remote vlan vlan-id reflector-port unit/slot/port}
```

**Mode**

Global Config

4.23.3 monitor session filter
This command attaches an IP/MAC ACL to a selected monitor session. This command configures a probe port and a monitored port for monitor session (port monitoring).

An IP/MAC ACL can be attached to a session by giving the access list number/name.

Use the `filter` parameter to filter a specified access group either by IP address or MAC address.

The commands described below add a mirrored port (source port) to a session identified with `session-id`. The `session-id` parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

---

**NOTICE**

Source and destination cannot be configured as remote on the same device.

---

**NOTICE**

IP/MAC ACL can be attached to a session by giving the access list number/name. On the platforms that do not support both IP and MAC ACLs to be assigned on the same Monitor session, an error message is thrown when user tries to configure ACLs of both types.

---

**Default**

None

**Format**

```
monitor session session-id filter {ip access-group acl-id/aclname | mac access-group acl-name}
```

**Mode**

Global Config
4.23.3.1 no monitor session filter

This command removes the specified IP/MAC ACL from the selected monitoring session.

Format

```
no smonitor session session-id filter {ip access-group | mac access-group }
```

Mode

Global Config

4.23.4 monitor session mode

This command enables the selected port mirroring session. This command configures a probe port and a monitored port for monitor session (port monitoring).

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

**NOTICE**

Source and destination cannot be configured as remote on the same device.

The commands described below add a mirrored port (source port) to a session identified with session-id. The session-id parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS. Option rx is used to monitor only ingress packets. Option tx is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

**NOTICE**

If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

**NOTICE**

Source and destination cannot be configured as remote on the same device.

**NOTICE**

On the intermediate switch: RSPAN VLAN should be created, the ports connected towards the Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on interface on intermediate switch connected towards Destination switch.

Default

None

Format

```
monitor session session-id mode
```

Mode

Global Config
4.23.4.1  no monitor session mode

This command disables the selected port mirroring session.

Format  

```
no monitor session session-id mode
```

Mode  

Global Config

4.23.5  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 unit/slot/port` parameter or `destination interface` to remove the specified interface from the port monitoring session. Use the `mode` parameter to disable the administrative mode of the session.

Format  

```
no monitor session session-id {source {interface unit/slot/port | cpu | lag | vlan | remote vlan} | destination {interface | remote vlan | mode | filter {ip access-group | mac access-group}}}
```

Mode  

Global Config

4.23.6  no monitor

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

Default  

enabled

Format  

```
no monitor
```

Mode  

Global Config

4.23.7  show monitor session

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

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>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.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <code>session-id</code>. The possible values are Enabled and Disabled.</td>
</tr>
<tr>
<td>Probe Port</td>
<td>Probe port (destination port) for the session identified with <code>session-id</code>. If probe port is not set then this field is blank.</td>
</tr>
<tr>
<td>Src VLAN</td>
<td>All member ports of this VLAN are mirrored. If the source VLAN is not configured, this field is blank.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mirrored Port</td>
<td>The port that is configured as a mirrored port (source port) for the session identified with <code>session-id</code>. If no source port is configured for the session, this field is blank.</td>
</tr>
<tr>
<td>Ref. Port</td>
<td>This port carries all the mirrored traffic at the source switch.</td>
</tr>
<tr>
<td>Src RVLAN</td>
<td>The source VLAN is configured at the destination switch. If the remote VLAN is not configured, this field is blank.</td>
</tr>
<tr>
<td>Dst RVLAN</td>
<td>The destination VLAN is configured at the source switch. If the remote VLAN is not configured, this field is blank.</td>
</tr>
<tr>
<td>Type</td>
<td>Direction in which source port configured for port mirroring. Types are tx for transmitted packets and rx for receiving packets.</td>
</tr>
<tr>
<td>IP ACL</td>
<td>The IP access-list id or name attached to the port mirroring session.</td>
</tr>
<tr>
<td>MAC ACL</td>
<td>The MAC access-list name attached to the port mirroring session.</td>
</tr>
</tbody>
</table>

**Example:** Example 1:
```
(Switch)#show monitor session 1
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Admin Mode</th>
<th>Probe Port</th>
<th>Src VLAN</th>
<th>Mirrored Port</th>
<th>Ref Port</th>
<th>Src RVLAN</th>
<th>Dst RVLAN</th>
<th>Type</th>
<th>IP ACL</th>
<th>MAC ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable</td>
<td>1/0/8</td>
<td></td>
<td>1/0/10</td>
<td>Rx, Tx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:** Example 2:
```
(Switch)#show monitor session all
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Admin Mode</th>
<th>Probe Port</th>
<th>Src VLAN</th>
<th>Mirrored Port</th>
<th>Ref Port</th>
<th>Src RVLAN</th>
<th>Dst RVLAN</th>
<th>Type</th>
<th>IP ACL</th>
<th>MAC ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable</td>
<td>1/0/8</td>
<td></td>
<td>1/0/10</td>
<td>Rx, Tx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Disable</td>
<td>6</td>
<td>0/4</td>
<td>10</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Disable</td>
<td>1/0/11</td>
<td></td>
<td>10</td>
<td>101</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Enable</td>
<td>1/0/11</td>
<td></td>
<td>1/0/7</td>
<td>Tx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:** Example 3:
```
(Switch)#show monitor session all
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Admin Mode</th>
<th>Probe Port</th>
<th>Src VLAN</th>
<th>Mirrored Port</th>
<th>Ref Port</th>
<th>Src RVLAN</th>
<th>Dst RVLAN</th>
<th>Type</th>
<th>IP ACL</th>
<th>MAC ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable</td>
<td>1/0/8</td>
<td></td>
<td>1/0/10</td>
<td>Rx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Enable</td>
<td>6</td>
<td></td>
<td></td>
<td>Rx</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Disable</td>
<td>10</td>
<td></td>
<td></td>
<td>Tx</td>
<td>101</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Disable</td>
<td>1/0/11</td>
<td></td>
<td>1/0/7</td>
<td>Tx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:** Example 4:
```
(Switch)#show monitor session all
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Admin Mode</th>
<th>Probe Port</th>
<th>Src VLAN</th>
<th>Mirrored Port</th>
<th>Ref Port</th>
<th>Src RVLAN</th>
<th>Dst RVLAN</th>
<th>Type</th>
<th>IP ACL</th>
<th>MAC ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable</td>
<td>1/0/15</td>
<td>1/0/4</td>
<td>11</td>
<td>Tx</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Enable</td>
<td>1/0/3</td>
<td></td>
<td>1/0/15</td>
<td>Tx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Enable</td>
<td>1/0/15</td>
<td>1/0/20</td>
<td>10</td>
<td>Rx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Enable</td>
<td>1/0/11</td>
<td></td>
<td>1/0/15</td>
<td>Rx</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example: Example 5:

(Switch)#show monitor session all

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Admin Mode</th>
<th>Probe Port</th>
<th>Src VLAN</th>
<th>Mirrored Port</th>
<th>Ref Port</th>
<th>Src RVLAN</th>
<th>Dst RVLAN</th>
<th>Type</th>
<th>IP ACL</th>
<th>MAC ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Disable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Enable</td>
<td>1/0/16</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Enable</td>
<td>1/0/11</td>
<td>1/0/16</td>
<td></td>
<td></td>
<td>Rx,Tx</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example: Example 6:

(Switch)#show monitor session all

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Admin Mode</th>
<th>Probe Port</th>
<th>Src VLAN</th>
<th>Mirrored Port</th>
<th>Ref Port</th>
<th>Src RVLAN</th>
<th>Dst RVLAN</th>
<th>Type</th>
<th>IP ACL</th>
<th>MAC ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable</td>
<td>1</td>
<td>1/0/4</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Enable</td>
<td>1/0/15</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Enable</td>
<td>3</td>
<td>1/0/20</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Enable</td>
<td>1/0/11</td>
<td>1/0/16</td>
<td></td>
<td></td>
<td>Rx,Tx</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.23.8 show vlan remote-span

This command displays the configured RSPAN VLAN.

Format: show vlan remote-span

Mode: Privileged EXEC Mode

Example: The following shows example output for the command.

(Switch)# show vlan remote-span

Remote SPAN VLAN

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100,102,201,303</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.24 Static MAC Filtering Commands

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.

4.24.1 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

### 4.24.1 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

### 4.24.2 macfilter adddest

Use this command to add the interface or range of 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.

**Format**  
```
macfilter adddest macaddr
```

**Mode**  
Interface Config

#### 4.24.2.1 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

### 4.24.3 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.

**Format**  
```
macfilter adddest all macaddr
```

**Mode**  
Global Config

---

**NOTICE**

Configuring a destination port list is only valid for multicast MAC addresses.
4.24.3.1 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

4.24.4 macfilter addsrc

This command adds the interface or range of interfaces 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

4.24.4.1 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

4.24.5 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

4.24.5.1 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

4.24.6 show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you specify `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
### 4.24.7 show mac-address-table staticfiltering

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

**Format**

```
show mac-address-table staticfiltering
```

**Mode**

Privileged EXEC

---

**Term** | **Definition**
---|---
MAC Address | The MAC Address of the static MAC filter entry.
VLAN ID | The VLAN ID of the static MAC filter entry.
Source Port(s) | The source port filter set’s slot and port(s).

---

**NOTICE**

Only multicast address filters will have destination port lists.

---

### 4.25 DHCP L2 Relay Agent Commands

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

#### 4.25.1 dhcp l2relay

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

**Format**

```
dhcp l2relay
```

**Mode**

- Global Config
- Interface Config

#### 4.25.1.1 no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

**Format**

```
no dhcp l2relay
```

**Mode**

- Global Config
- Interface Config
4.25.2  dhcp l2relay circuit-id subscription

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

**Default**  disabled

**Format**  dhcp l2relay circuit-id subscription *subscription-string*

**Mode**  Interface Config

4.25.2.1  no dhcp l2relay circuit-id subscription

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

**Format**  no dhcp l2relay circuit-id subscription *subscription-string*

**Mode**  Interface Config

4.25.3  dhcp l2relay circuit-id vlan

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

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

**Mode**  Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.</td>
</tr>
</tbody>
</table>

4.25.3.1  no dhcp l2relay circuit-id vlan

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

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

**Mode**  Global Config

4.25.4  dhcp l2relay remote-id subscription

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

**Default**  empty string

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

**Mode**  Interface Config
4.25.4.1 no dhcp l2relay remote-id subscription

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

Format
no dhcp l2relay remote-id remoteid-string subscription-name subscription-string

Mode
Interface Config

4.25.5 dhcp l2relay remote-id vlan

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

Format
dhcp l2relay remote-id remote-id-string vlan vlan-list

Mode
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.</td>
</tr>
</tbody>
</table>

4.25.5.1 no dhcp l2relay remote-id vlan

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

Format
no dhcp l2relay remote-id vlan vlan-list

Mode
Global Config

4.25.6 dhcp l2relay subscription

This command enables relaying DHCP packets on an interface or range of interfaces that fall under the specified service subscription. The subscription-string is a character string that needs to be matched with configured DOT1AD subscription string for correct operation.

Default
disabled (i.e. no DHCP packets are relayed)

Format
dhcp l2relay subscription-name subscription-string

Mode
Interface Config

4.25.6.1 no dhcp l2relay subscription

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

Format
no dhcp l2relay subscription-name subscription-string

Mode
Interface Config

4.25.7 dhcp l2relay trust

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

Default
untrusted

Format
dhcp l2relay trust

Mode
Interface Config
4.25.7.1  no dhcp l2relay trust
Use this command to configure an interface to the default untrusted for Option-82 reception.

Format    no dhcp l2relay trust
Mode       Interface Config

4.25.8  dhcp l2relay vlan
Use this command to enable the DHCP L2 Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default   disable
Format     dhcp l2relay vlan vlan-list
Mode       Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>The VLAN ID. The range is 1–4093. Separate nonconsecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.</td>
</tr>
</tbody>
</table>

4.25.8.1  no dhcp l2relay vlan
Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Format     no dhcp l2relay vlan vlan-list
Mode        Global Config

4.25.9  show dhcp l2relay all
This command displays the summary of DHCP L2 Relay configuration.

Format     show dhcp l2relay all
Mode        Privileged EXEC

Example: The following shows example CLI display output for the command.
(FASTPATH Switching) #show dhcp l2relay all

DHCP L2 Relay is Enabled.

<table>
<thead>
<tr>
<th>Interface</th>
<th>L2RelayMode</th>
<th>TrustMode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/2</td>
<td>Enabled</td>
<td>untrusted</td>
</tr>
<tr>
<td>0/4</td>
<td>Disabled</td>
<td>trusted</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>L2 Relay</th>
<th>CircuitId</th>
<th>RemoteId</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Disabled</td>
<td>Enabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>5</td>
<td>Enabled</td>
<td>Enabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>6</td>
<td>Enabled</td>
<td>Enabled</td>
<td>broadband</td>
</tr>
<tr>
<td>7</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>8</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>9</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>10</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
</tr>
</tbody>
</table>
4.25.10  show dhcp l2relay circuit-id vlan

This command displays DHCP circuit-id vlan configuration.

**Format**  
show dhcp l2relay circuit-id vlan vlan-list

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.</td>
</tr>
</tbody>
</table>

4.25.11  show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

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

**Mode**  
Privileged EXEC

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

(FASTPATH Switching) #show dhcp l2relay interface all

DHCP L2 Relay is Enabled.

<table>
<thead>
<tr>
<th>Interface</th>
<th>L2RelayMode</th>
<th>TrustMode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/2</td>
<td>Enabled</td>
<td>untrusted</td>
</tr>
<tr>
<td>0/4</td>
<td>Disabled</td>
<td>trusted</td>
</tr>
</tbody>
</table>

4.25.12  show dhcp l2relay remote-id vlan

This command displays DHCP Remote-id vlan configuration.

**Format**  
show dhcp l2relay remote-id vlan vlan-list

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.</td>
</tr>
</tbody>
</table>

4.25.13  show dhcp l2relay stats interface

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

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

**Mode**  
Privileged EXEC

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

(FASTPATH Switching) #show dhcp l2relay stats interface all

DHCP L2 Relay is Enabled.

<table>
<thead>
<tr>
<th>Interface</th>
<th>UntrustedServer</th>
<th>UntrustedClient</th>
<th>TrustedServer</th>
<th>TrustedClient</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MsgsWithOpt82</td>
<td>MsgsWithOpt82</td>
<td>MsgsWithoutOpt82</td>
<td>MsgsWithoutOpt82</td>
</tr>
</tbody>
</table>
### 4.25.14 show dhcp l2relay subscription interface

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

**Format**

```
show dhcp l2relay subscription interface {all|interface-num}
```

**Mode**

Privileged EXEC

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

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

+-----------------+-----------------+-----------+-----------+-----------------+-----------+-----------------+-----------+
<table>
<thead>
<tr>
<th>Interface</th>
<th>SubscriptionName</th>
<th>L2Relay</th>
<th>Circuit</th>
<th>Remote</th>
<th>mode</th>
<th>L2Relay Circuit</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>sub1</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
<td></td>
<td>--NULL--</td>
<td></td>
</tr>
<tr>
<td>0/2</td>
<td>sub3</td>
<td>Enabled</td>
<td>Disabled</td>
<td>EnterpriseSwitch</td>
<td></td>
<td>--NULL--</td>
<td></td>
</tr>
<tr>
<td>0/2</td>
<td>sub22</td>
<td>Disabled</td>
<td>Enabled</td>
<td>--NULL--</td>
<td></td>
<td>--NULL--</td>
<td></td>
</tr>
<tr>
<td>0/4</td>
<td>sub4</td>
<td>Enabled</td>
<td>Enabled</td>
<td>--NULL--</td>
<td></td>
<td>--NULL--</td>
<td></td>
</tr>
</tbody>
</table>
```

### 4.25.15 show dhcp l2relay agent-option vlan

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

**Format**

```
show dhcp l2relay agent-option vlan vlan-range
```

**Mode**

Privileged EXEC

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

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

DHCP L2 Relay is Enabled.

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>L2 Relay</th>
<th>CircuitId</th>
<th>RemoteId</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Enabled</td>
<td>Enabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>6</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Broadcom</td>
</tr>
<tr>
<td>7</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>8</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>9</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
</tr>
<tr>
<td>10</td>
<td>Enabled</td>
<td>Disabled</td>
<td>--NULL--</td>
</tr>
</tbody>
</table>
```
4.25.16  show dhcp l2relay vlan
This command displays DHCP vlan configuration.

Format  show dhcp l2relay vlan vlan-list
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-list</td>
<td>Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.</td>
</tr>
</tbody>
</table>

4.25.17  clear dhcp l2relay statistics interface
Use this command to reset the DHCP L2 relay counters to zero. Specify the port with the counters to clear, or use the all keyword to clear the counters on all ports.

Format  clear dhcp l2relay statistics interface {slot/port | all}
Mode    Privileged EXEC

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

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

Format  dhcp client vendor-id-option string
Mode    Global Config

4.26.1.1  no dhcp client vendor-id-option
This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the FASTPATH switch.

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

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

Format  dhcp client vendor-id-option-string string
Mode    Global Config
4.26.2.1 no dhcp client vendor-id-option-string
This parameter clears the DHCP Vendor Option-60 string.

**Format**
no dhcp client vendor-id-option-string

**Mode**
Global Config

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

**Format**
show dhcp client vendor-id-option

**Mode**
Privileged EXEC

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

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

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

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

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

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

**Mode**
Interface Config

4.26.4.1 no ip dhcp force-client-id
This command disables the manipulation of a DHCP packet.

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

**Mode**
Interface Config
4.26.5  **show ip dhcp force-client-id**
This command displays the mode (enabled/disabled) and the related VLAN and client-identifier for a specified interface (<unit/slot/port>) or for all physical interfaces.

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

**Mode**  
Privileged Exec

4.26.6  **clear ip dhcp force-client-id**
This command clears all configured manipulation rules for DHSP packets for all interfaces.

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

**Mode**  
Privileged Exec

### 4.27 DHCP Snooping Configuration Commands
This section describes commands you use to configure DHCP Snooping.

#### 4.27.1  **ip dhcp snooping**
Use this command to enable DHCP Snooping globally.

**Default**  
disabled

**Format**  
ip dhcp snooping

**Mode**  
Global Config

#### 4.27.1.1  **no ip dhcp snooping**
Use this command to disable DHCP Snooping globally.

**Format**  
no ip dhcp snooping

**Mode**  
Global Config

#### 4.27.2  **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
4.27.2.1 *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
```

4.27.3 *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
```

4.27.3.1 *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
```

4.27.4 *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
```

4.27.5 *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
```
4.27.5.1 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

4.27.6 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

4.27.6.1 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

4.27.7 ip dhcp filtering trust
Use this command to enable trusted mode on the interface if the previously saved configuration or applied script contains this command.

Format: ip dhcp filtering trust interface id
Mode: Global Config

4.27.7.1 no ip dhcp filtering trust
Use this command to disable trusted mode on the interface.

Format: no ip dhcp filtering trust interface id
Mode: Global Config

4.27.8 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

4.27.8.1 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
4.27.9  ip dhcp snooping limit
Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second. The burst level range is 1 to 15 seconds.

Default: disabled (no limit)

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

Mode: Interface Config

4.27.9.1  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

4.27.10  ip dhcp snooping log-invalid
Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default: disabled

Format: `ip dhcp snooping log-invalid`

Mode: Interface Config

4.27.10.1  no ip dhcp snooping log-invalid
Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format: `no ip dhcp snooping log-invalid`

Mode: Interface Config

4.27.11  ip dhcp snooping trust
Use this command to configure an interface or range of interfaces as trusted.

Default: disabled

Format: `ip dhcp snooping trust`

Mode: Interface Config
4.27.11 no ip dhcp snooping trust
Use this command to configure the port as untrusted.

Format no ip dhcp snooping trust
Mode Interface Config

4.27.12 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.
This command can be used to configure a single interface or a range of interfaces.

Default the source ID is the IP address
Format ip verify source {port-security}
Mode Interface Config

4.27.12.1 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.

Format no ip verify source
Mode Interface Config

4.27.13 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

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

**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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Log Invalid Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>0/2</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>0/3</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>0/4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0/6</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```
4.27.14 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the valid IP address for the binding rule.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN for the binding rule.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface to add a binding into the DHCP snooping interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Binding type; statically configured from the CLI or dynamically learned.</td>
</tr>
<tr>
<td>Lease (sec)</td>
<td>The remaining lease time for the entry.</td>
</tr>
</tbody>
</table>

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

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

Total number of bindings: 2

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>VLAN</th>
<th>Interface</th>
<th>Type</th>
<th>Lease time (Secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:B3:06:60:80</td>
<td>210.1.1.3</td>
<td>10</td>
<td>0/1</td>
<td></td>
<td>86400</td>
</tr>
<tr>
<td>00:0F:FE:00:13:04</td>
<td>210.1.1.4</td>
<td>10</td>
<td>0/1</td>
<td></td>
<td>86400</td>
</tr>
</tbody>
</table>

4.27.15 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent URL</td>
<td>Bindings database agent URL.</td>
</tr>
<tr>
<td>Write Delay</td>
<td>The maximum write time to write the database into local or remote.</td>
</tr>
</tbody>
</table>

**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
4.27.16  show ip dhcp snooping interfaces
Use this command to show the DHCP Snooping status of the interfaces.

**Format**  
show ip dhcp snooping interfaces

**Mode**  
Privileged EXEC

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

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust</th>
<th>State</th>
<th>Rate Limit</th>
<th>Burst Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>(pps)</td>
<td>(seconds)</td>
</tr>
<tr>
<td>1/g1</td>
<td>No</td>
<td>15</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1/g2</td>
<td>No</td>
<td>15</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1/g3</td>
<td>No</td>
<td>15</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
```

```
(switch) #show ip dhcp snooping interfaces ethernet 1/g15

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust</th>
<th>Rate Limit</th>
<th>Burst Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(pps)</td>
<td>(seconds)</td>
</tr>
<tr>
<td>1/g15</td>
<td>Yes</td>
<td>15</td>
<td>1</td>
</tr>
</tbody>
</table>
```

4.27.17  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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The IP address of the interface in <em>slot/port</em> format.</td>
</tr>
<tr>
<td>MAC Verify Failures</td>
<td>Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.</td>
</tr>
<tr>
<td>Client Ifc Mismatch</td>
<td>Represents the number of DHCP release and Deny messages received on the different ports than learned previously.</td>
</tr>
<tr>
<td>DHCP Server Msgs Rec'd</td>
<td>Represents the number of DHCP server messages received on Untrusted ports.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Verify Failures</th>
<th>Client Ifc Mismatch</th>
<th>DHCP Server Msgs Rec'd</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
4.27.18  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

4.27.19  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

4.27.20  show ip verify source
Use this command to display the IPSG configurations on all ports.

Format  show ip verify source
Mode     • Privileged EXEC
         • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface address in slot/port format.</td>
</tr>
<tr>
<td>Filter Type</td>
<td>Is one of two values:</td>
</tr>
<tr>
<td></td>
<td>• ip-mac: User has configured MAC address filtering on this interface.</td>
</tr>
<tr>
<td></td>
<td>• ip: Only IP address filtering on this interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the interface</td>
</tr>
<tr>
<td>MAC Address</td>
<td>If MAC address filtering is not configured on the interface, the MAC Address</td>
</tr>
<tr>
<td></td>
<td>field is empty. If port security is disabled on the interface, then the</td>
</tr>
<tr>
<td></td>
<td>MAC Address field displays “permit-all.”</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN for the binding rule.</td>
</tr>
</tbody>
</table>

**Example:** The following shows example CLI display output for the command.
```
(switch) #show ip verify source
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter Type</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>ip-mac</td>
<td>210.1.1.3</td>
<td>00:02:B3:06:60:80</td>
<td>10</td>
</tr>
<tr>
<td>0/1</td>
<td>ip-mac</td>
<td>210.1.1.4</td>
<td>00:0F:FE:00:13:04</td>
<td>10</td>
</tr>
</tbody>
</table>
### 4.27.21 show ip verify interface

Use this command to display the IPSG filter type for a specific interface.

**Format**

```
show ip verify interface slot/port
```

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface address in <code>slot/port</code> format.</td>
</tr>
</tbody>
</table>
| Filter Type| Is one of two values:  
  - `ip-mac`: User has configured MAC address filtering on this interface.  
  - `ip`: Only IP address filtering on this interface.                       |

### 4.27.22 show ip source binding

Use this command to display the IPSG bindings.

**Format**

```
show ip source binding [{dhcp-snooping|static}] [interface slot/port] [vlan id]
```

**Mode**

- Privileged EXEC
- User EXEC

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

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

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

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:08</td>
<td>1.2.3.4</td>
<td>dhcp-snooping</td>
<td>2</td>
<td>0/1</td>
</tr>
<tr>
<td>00:00:00:00:00:00:09</td>
<td>1.2.3.4</td>
<td>dhcp-snooping</td>
<td>3</td>
<td>0/1</td>
</tr>
<tr>
<td>00:00:00:00:00:00:00:8A</td>
<td>1.2.3.4</td>
<td>dhcp-snooping</td>
<td>4</td>
<td>0/1</td>
</tr>
</tbody>
</table>

### 4.28 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.
4.28.1  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

4.28.1.1  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

4.28.2  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

4.28.2.1  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

4.28.3  ip arp inspection vlan logging
Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default: enabled
Format: ip arp inspection vlan vlan-list logging
Mode: Global Config
4.28.3.1 no ip arp inspection vlan logging
Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

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

4.28.4 ip arp inspection trust
Use this command to configure an interface or range of interfaces as trusted for Dynamic ARP Inspection.

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

4.28.4.1 no ip arp inspection trust
Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format: no ip arp inspection trust
Mode: Interface Config

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

```
[NOTICE] The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.
```

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

4.28.5.1 no ip arp inspection limit
Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format: no ip arp inspection limit
Mode: Interface Config
4.28.6  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

4.28.6.1  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

4.28.7  arp access-list
Use this command to create an ARP ACL.

Format             arp access-list acl-name
Mode               Global Config

4.28.7.1  no arp access-list
Use this command to delete a configured ARP ACL.

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

4.28.8  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
4.28.8.1 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

4.28.9 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source MAC Validation</td>
<td>Displays whether Source MAC Validation of ARP frame is enabled or disabled.</td>
</tr>
<tr>
<td>Destination MAC Validation</td>
<td>Displays whether Destination MAC Validation is enabled or disabled.</td>
</tr>
<tr>
<td>IP Address Validation</td>
<td>Displays whether IP Address Validation is enabled or disabled.</td>
</tr>
<tr>
<td>VLAN Configuration</td>
<td>The VLAN ID for each displayed row.</td>
</tr>
<tr>
<td>Log Invalid</td>
<td>Displays whether logging of invalid ARP packets is enabled on the VLAN.</td>
</tr>
<tr>
<td>ACL Name</td>
<td>The ARP ACL Name, if configured on the VLAN.</td>
</tr>
<tr>
<td>Static Flag</td>
<td>If the ARP ACL is configured static on the VLAN.</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the command.
```
(switch) #show ip arp inspection vlan 10-12
```

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

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Configuration</th>
<th>Log Invalid</th>
<th>ACL Name</th>
<th>Static flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Enabled</td>
<td>Enabled</td>
<td>H2</td>
<td>Enabled</td>
</tr>
<tr>
<td>11</td>
<td>Disabled</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Enabled</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.28.10 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
**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.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Forwarded</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>90</td>
<td>14</td>
</tr>
<tr>
<td>20</td>
<td>10</td>
<td>3</td>
</tr>
</tbody>
</table>

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

```
<table>
<thead>
<tr>
<th>VLAN</th>
<th>DHCP Drops</th>
<th>ACL Drops</th>
<th>DHCP Permits</th>
<th>ACL Permits</th>
<th>Bad Src MAC</th>
<th>Bad Dest MAC</th>
<th>Invalid MAC</th>
<th>Invalid IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>11</td>
<td>1</td>
<td>65</td>
<td>25</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>0</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
```

### 4.28.11 clear ip arp inspection statistics

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

**Default** none

**Format** `clear ip arp inspection statistics`

**Mode** Privileged EXEC

### 4.28.12 show ip arp inspection interfaces

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

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

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface ID for each displayed row.</td>
</tr>
<tr>
<td>Trust State</td>
<td>Whether the interface is trusted or untrusted for DAI.</td>
</tr>
<tr>
<td>Rate Limit</td>
<td>The configured rate limit value in packets per second.</td>
</tr>
<tr>
<td>Burst Interval</td>
<td>The configured burst interval value in seconds.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(switch) #show ip arp inspection interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate Limit (pps)</th>
<th>Burst Interval (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Untrusted</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>0/2</td>
<td>Untrusted</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

4.28.13 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.

(switch) #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

4.29 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.

This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

4.29.1 set igmp

This command enables IGMP Snooping on the system (Global Config Mode), an interface, or a range of interfaces. 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.
4.29.1.1  no set igmp
This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN.

Format  no set igmp [vlan_id]
Mode    •  Global Config
        •  Interface Config
        •  VLAN Config

4.29.2  set igmp header-validation
This command enables header validation for IGMP messages.
When header validation is enabled, IGMP Snooping checks:
•  The time-to-live(TTL) field in the IGMP header and drops packets where TTL is not equal to 1. The TTL field should always be set to 1 in the headers of IGMP reports and queries.
•  The presence of the router alert option (9404) in the IP packet header of the IGMPv2 message and drops packets that do not include this option.
•  The presence of the router alert option (9404) and ToS Byte = 0xC0 (Internet Control) in the IP packet header of IGMPv3 message and drops packets that do not include these options.

Default  enabled
Format    set igmp header-validation
Mode      Global Config

4.29.2.1  no set igmp header-validation
This command disables header validation for IGMP messages.

Format  no set igmp header-validation
Mode    Global Config

4.29.3  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
4.29.3.1 no set igmp interfacemode
This command disables IGMP Snooping on all interfaces.

Format          no set igmp interfacemode
Mode            Global Config

4.29.4 set igmp fast-leave
This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface, a range of interfaces, or a 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 [vlan_id]
Mode            Interface Config
                Interface Range
                VLAN Config

4.29.4.1 no set igmp fast-leave
This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format          no set igmp fast-leave [vlan_id]
Mode            Interface Config
                Interface Range
                VLAN Config

4.29.5 set igmp groupmembership-interval
This command sets the IGMP Group Membership Interval time on a VLAN, one interface, a range of interfaces, 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 [vlan_id] 2-3600
Mode            • Interface Config
                • Global Config
                • VLAN Config
4.29.5.1  no set igmp groupmembership-interval

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

**Format**
```
no set igmp groupmembership-interval [vlan_id]
```

**Mode**
- Interface Config
- Global Config
- VLAN Config

4.29.6  set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. 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 [vlan_id] 1-25
```

**Mode**
- Global Config
- Interface Config
- VLAN Config

4.29.6.1  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 [vlan_id]
```

**Mode**
- Global Config
- Interface Config
- VLAN Config

4.29.7  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, or on a range of interfaces. 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 [vlan_id] 0-3600
```

**Mode**
- Global Config
- Interface Config
- VLAN Config
4.29.7.1  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 [vlan_id]
Mode:    • Global Config
         • Interface Config
         • VLAN Config

Format:  no set igmp mcrtrexpiretime vlan_id
Mode:    VLAN Config

4.29.8  set igmp mrouter
This command configures the VLAN ID (vlan_id) that has the multicast router mode enabled.

Format:  set igmp mrouter vlan_id
Mode:    Interface Config

4.29.8.1 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

4.29.9  set igmp mrouter interface
This command configures the interface or range of interfaces 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

4.29.9.1 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
4.29.10 set igmp report-suppression

Use this command to suppress the IGMP reports on a given VLAN ID. In order to optimize the number of reports traversing the network with no added benefits, a Report Suppression mechanism is implemented. When more than one client responds to an MGMD query for the same Multicast Group address within the max-response-time, only the first response is forwarded to the query and others are suppressed at the switch.

**Default** Disabled

**Format** `set igmp report-suppression vlan-id`

**Mode** VLAN Config

---

**Example:** The following shows an example of the command.

```
(FASTPATH Switching) #vlan database
(FASTPATH Switching) (Vlan)#set igmp report-suppression ?
<1-4093> Enter VLAN ID.
(FASTPATH Switching) (Vlan)#set igmp report-suppression 1
```

4.29.10.1 no set igmp report-suppression

Use this command to return the system to the default.

**Format** `no set igmp report-suppression`

**Mode** VLAN Config

4.29.11 show igmpsnooping

This command displays IGMP Snooping information for a given slot/port or VLAN. 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:

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

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping Admin Mode</td>
<td>Indicates whether IGMP Snooping is active on the interface.</td>
</tr>
<tr>
<td>Fast Leave Mode</td>
<td>Indicates whether IGMP Snooping Fast-leave is active on the interface.</td>
</tr>
</tbody>
</table>
When you specify a value for `vlan_id`, the following information appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Membership Interval</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Maximum Response Time</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Multicast Router Expiry Time</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Switching) #show igmpsnooping 1

```
VLAN ID........................................ 1
IGMP Snooping Admin Mode................. Disabled
Fast Leave Mode............................ Disabled
Group Membership Interval (secs)......... 260
Max Response Time (secs).................. 10
Multicast Router Expiry Time (secs).... 0
Report Suppression Mode.................. Enabled
```

4.29.12  **show igmpsnooping mrouter interface**

This command displays information about statically configured ports.

**Format**

```
show igmpsnooping mrouter interface slot/port
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>The port on which multicast router information is being displayed.</td>
</tr>
<tr>
<td><strong>Multicast Router Attached</strong></td>
<td>Indicates whether multicast router is statically enabled on the interface.</td>
</tr>
<tr>
<td><strong>VLAN ID</strong></td>
<td>The list of VLANs of which the interface is a member.</td>
</tr>
</tbody>
</table>
4.29.13  show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

**Format**

```
show igmpsnooping mrouter vlan slot/port
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The port on which multicast router information is being displayed.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The list of VLANs of which the interface is a member.</td>
</tr>
</tbody>
</table>

4.29.14  show igmpsnooping ssm

This command displays information about Source Specific Multicasting (SSM) by entry, group, or statistics. SSM delivers multicast packets to receivers that originated from a source address specified by the receiver. SSM is only available with IGMPv3 and MLDv2.

**Format**

```
show igmpsnooping ssm {entries | groups | stats}
```

**Mode**

Privileged EXEC

4.29.15  show mac-address-table igmpsnooping

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

**Format**

```
show mac-address-table igmpsnooping
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN in which the MAC address is learned.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.</td>
</tr>
<tr>
<td>Type</td>
<td>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).</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of this multicast table entry.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).</td>
</tr>
</tbody>
</table>

4.29.16  ip dhcp force-client-id

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

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

**Format**

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

**Mode**

Interface Config
4.29.16.1 no ip dhcp force-client-id

This command disables the manipulation of a DHCP packet.

Format

no ip dhcp force-client-id

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

Mode Interface Config

4.29.17 show ip dhcp force-client-id

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

Format

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

Mode Privileged Exec

4.29.18 clear ip dhcp force-client-id

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

Format clear ip dhcp force-client-id

Mode Privileged Exec

4.30 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.

This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

4.30.1 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.

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.
4.30.1 no set igmp querier

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

Format
no set igmp querier [vlan-id] [address ipv4_address]

Mode
• Global Config
• VLAN Mode

4.30.2 set igmp querier query-interval

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

Default disabled

Format set igmp querier query-interval 1-1800

Mode Global Config

4.30.2.1 no set igmp querier query-interval

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

Format no set igmp querier query-interval

Mode Global Config

4.30.3 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
4.30.3.1 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

4.30.4 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

4.30.4.1 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

4.30.5 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

4.30.5.1 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

4.30.6 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 \texttt{vlanid} is not used, the command displays the following information.

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

When you specify a value for \texttt{vlanid}, the following additional information appears.

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

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

### 4.31 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.

\begin{center}
\textbf{NOTICE}
\end{center}

This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.
4.31.1 set mld
This command enables MLD Snooping on the system (Global Config Mode) or an Interface (Interface Config Mode). This command also enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.

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

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

Default disabled
Format set mld vlanid
Mode • Global Config
• Interface Config
• VLAN Mode

4.31.1.1 no set mld
Use this command to disable MLD Snooping on the system.

Format set mld vlanid
Mode • Global Config
• Interface Config
• VLAN Mode

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

Default disabled
Format set mld interfacemode
Mode Global Config

4.31.2.1 no set mld interfacemode
Use this command to disable MLD Snooping on all interfaces.

Format no set mld interfacemode
Mode Global Config
4.31.3  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.

**NOTICE**

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.

**NOTICE**

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

**Default**  disabled  
**Format**  set mld fast-leave vlanid 
**Mode**  
  * Interface Config  
  * VLAN Mode

4.31.3.1  no set mld fast-leave

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

**Format**  no set mld fast-leave vlanid 
**Mode**  
  * Interface Config  
  * VLAN Mode

4.31.4  set mld groupmembership-interval

Use this command to set the MLD Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

**Default**  260 seconds  
**Format**  set mld groupmembership-interval vlanid 2-3600  
**Mode**  
  * Interface Config  
  * Global Config  
  * VLAN Mode
4.31.4.1 no set groupmembership-interval
Use this command to set the MLDv2 Group Membership Interval time to the default value.

Format
no set mld groupmembership-interval

Mode
• Interface Config
• Global Config
• VLAN Mode

4.31.5 set mld maxresponse
Use this command to set the MLD Maximum Response time for the system, on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Query Interval time value. The range is 1 to 65 seconds.

Default
10 seconds

Format
set mld maxresponse 1-65

Mode
• Global Config
• Interface Config
• VLAN Mode

4.31.5.1 no set mld maxresponse
Use this command to set the max response time (on the interface or VLAN) to the default value.

Format
no set mld maxresponse

Mode
• Global Config
• Interface Config
• VLAN Mode

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

Default
0

Format
set mld mcrtexpiretime vlanid 0-3600

Mode
• Global Config
• Interface Config
4.31.6.1 no set mld mcrtexpiretime
Use this command to set the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format
   no set mld mcrtexpiretime vlanid
Mode
   • Global Config
   • Interface Config

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

Format
   set mld mrouter vlanid
Mode
   Interface Config

4.31.7.1 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

4.31.8 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

4.31.8.1 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

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

Format
   show mldsnooping [slot/port | vlanid]
Mode
   Privileged EXEC
When the optional arguments slot/port or `vlanid` are not used, the command displays the following information.

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

When you specify the slot/port values, the following information displays.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLD Snooping Admin Mode</td>
<td>Indicates whether MLD Snooping is active on the interface.</td>
</tr>
<tr>
<td>Fast Leave Mode</td>
<td>Indicates whether MLD Snooping Fast Leave is active on the VLAN.</td>
</tr>
<tr>
<td>Group Membership Interval</td>
<td>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.</td>
</tr>
<tr>
<td>Max Response Time</td>
<td>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.</td>
</tr>
<tr>
<td>Multicast Router Present Expiration Time</td>
<td>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.</td>
</tr>
</tbody>
</table>

When you specify a value for `vlanid`, the following information appears.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Admin Mode</td>
<td>Indicates whether MLD Snooping is active on the VLAN.</td>
</tr>
</tbody>
</table>
4.31.10  show mldsnooping mrouter interface
Use this command to display information about statically configured multicast router attached interfaces.

Format  show mldsnooping mrouter interface slot/port
Mode    Privileged EXEC

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

4.31.11  show mldsnooping mrouter vlan
Use this command to display information about statically configured multicast router-attached interfaces.

Format  show mldsnooping mrouter vlan slot/port
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Shows the interface on which multicast router information is being displayed.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Displays the list of VLANs of which the interface is a member.</td>
</tr>
</tbody>
</table>

4.31.12  show mldsnooping ssm entries
Use this command to display the source specific multicast forwarding database built by MLD snooping.
A given {Source, Group, VLAN} combination can have few interfaces in INCLUDE mode and few interfaces in EXCLUDE mode. In such instances, two rows for the same {Source, Group, VLAN} combinations are displayed.

Format  show mldsnooping ssm entries
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>The VLAN on which the entry is learned.</td>
</tr>
<tr>
<td>Group</td>
<td>The IPv6 multicast group address.</td>
</tr>
<tr>
<td>Source</td>
<td>The IPv6 source address.</td>
</tr>
<tr>
<td>Source Filter Mode</td>
<td>The source filter mode (Include/Exclude) for the specified group.</td>
</tr>
</tbody>
</table>
| Interfaces                | 1) If Source Filter Mode is "Include," specifies the list of interfaces on which a incoming packet is forwarded. If it's source IP address is equal to the current entry's Source, the destination IP address is equal to the current entry's Group and the VLAN ID on which it arrived is current entry's VLAN.  
   2) If Source Filter Mode is "Exclude," specifies the list of interfaces on which a incoming packet is forwarded. If it's source IP address is "not" equal to the current entry's Source, the destination IP address is equal to current entry's Group and VLAN ID on which it arrived is current entry's VLAN. |
4.31.13  show mldsnooping ssm stats
Use this command to display the statistics of MLD snooping's SSMFDB. This command takes no options.

Format  show mldsnooping ssm stats
Mode   Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Entries</td>
<td>The total number of entries that can possibly be in the MLD snooping's SSMFDB.</td>
</tr>
<tr>
<td>Most SSMFDB Entries Ever Used</td>
<td>The largest number of entries that have been present in the MLD snooping's SSMFDB.</td>
</tr>
<tr>
<td>Current Entries</td>
<td>The current number of entries in the MLD snooping's SSMFDB.</td>
</tr>
</tbody>
</table>

4.31.14  show mldsnooping ssm groups
Use this command to display the MLD SSM group membership information.

Format  show mldsnooping ssm groups
Mode   Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN on which the MLD v2 report is received.</td>
</tr>
<tr>
<td>Group</td>
<td>The IPv6 multicast group address.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface on which the MLD v2 report is received.</td>
</tr>
<tr>
<td>Reporter</td>
<td>The IPv6 address of the host that sent the MLDv2 report.</td>
</tr>
<tr>
<td>Source Filter Mode</td>
<td>The source filter mode (Include/Exclude) for the specified group.</td>
</tr>
<tr>
<td>Source Address List</td>
<td>List of source IP addresses for which source filtering is requested.</td>
</tr>
</tbody>
</table>

4.31.15  show mac-address-table mldsnooping
Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format  show mac-address-table mldsnooping
Mode   Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN in which the MAC address is learned.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.</td>
</tr>
<tr>
<td>Type</td>
<td>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.)</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of this multicast table entry.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).</td>
</tr>
</tbody>
</table>
4.31.16 clear mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

**Format**
```
clear mldsnooping
```

**Mode**
Privileged EXEC

---

4.32 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.

**4.32.1 set mld querier**

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

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

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

**Default**
disabled

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

**Mode**
- Global Config
- VLAN Mode

**4.32.1.1 no set mld querier**

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

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

**Mode**
- Global Config
- VLAN Mode

**4.32.2 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**
60 seconds

**Format**
```
set mld querier query_interval 1-1800
```

**Mode**
Global Config
4.32.2.1 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

4.32.3 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

4.32.3.1 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

4.32.4 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

4.32.4.1 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

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

Format: `show mldsnooping querier [detail | vlan vlanid]`
Mode: Privileged EXEC
When the optional arguments `vlandid` are not used, the command displays the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>Indicates whether or not MLD Snooping Querier is active on the switch.</td>
</tr>
<tr>
<td>Admin Version</td>
<td>Indicates the version of MLD that will be used while sending out the queries. This is defaulted to MLD v1 and it cannot be changed.</td>
</tr>
<tr>
<td>Querier Address</td>
<td>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.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.</td>
</tr>
<tr>
<td>Querier Timeout</td>
<td>Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.</td>
</tr>
</tbody>
</table>

When you specify a value for `vlandid`, the following information appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Admin Mode</td>
<td>Indicates whether MLD Snooping Querier is active on the VLAN.</td>
</tr>
<tr>
<td>VLAN Operational State</td>
<td>Indicates whether MLD Snooping Querier is in &quot;Querier&quot; or &quot;Non-Querier&quot; state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.</td>
</tr>
<tr>
<td>VLAN Operational Max Response Time</td>
<td>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.</td>
</tr>
<tr>
<td>Querier Election Participate</td>
<td>Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.</td>
</tr>
<tr>
<td>Querier VLAN Address</td>
<td>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.</td>
</tr>
<tr>
<td>Operational Version</td>
<td>This version of IPv6 will be used while sending out MLD queries on this VLAN.</td>
</tr>
<tr>
<td>Last Querier Address</td>
<td>Indicates the IP address of the most recent Querier from which a Query was received.</td>
</tr>
<tr>
<td>Last Querier Version</td>
<td>Indicates the MLD version of the most recent Querier from which a Query was received on this VLAN.</td>
</tr>
</tbody>
</table>

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

### 4.33 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.

---

**Notice**

To enable the SNMP trap specific to port security, see “snmp-server enable traps violation” on page 72

---

### 4.33.1 port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default: disabled

**Format**

`port-security`

**Mode**

- Global Config (to enable port locking globally)
- Interface Config (to enable port locking on an interface or range of interfaces)
4.33.1  **no port-security**
This command disables port locking for one (Interface Config) or all (Global Config) ports.

**Format**
```
no port-security
```

**Mode**
- Global Config
- Interface Config

4.33.2  **port-security max-dynamic**
This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port. The valid range is 0–600.

**Default**
600

**Format**
```
port-security max-dynamic maxvalue
```

**Mode**
Interface Config

4.33.2.1  **no port-security max-dynamic**
This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

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

**Mode**
Interface Config

4.33.3  **port-security max-static**
This command sets the maximum number of statically locked MAC addresses allowed on a port. The valid range is 0–20.

**Default**
1

**Format**
```
port-security max-static maxvalue
```

**Mode**
Interface Config

4.33.3.1  **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

4.33.4  **port-security mac-address**
This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The **vid** is the VLAN ID.

**Format**
```
port-security mac-address mac-address vid
```

**Mode**
Interface Config
4.33.4.1 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

4.33.5 port-security mac-address move
This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format: port-security mac-address move
Mode: Interface Config

4.33.6 port-security mac-address sticky
This command enables sticky mode Port MAC Locking on a port. If accompanied by a MAC address and a VLAN id (for interface config mode only), it adds a sticky MAC address to the list of statically locked MAC addresses. These sticky addresses are converted back to dynamically locked addresses if sticky mode is disabled on the port. The <vid> is the VLAN ID. The Global command applies the "sticky" mode to all valid interfaces (physical and LAG). There is no global sticky mode as such.

Sticky addresses that are dynamically learned will appear in show running-config as "port-security mac-address sticky <mac> <vid>" entries. This distinguishes them from static entries.

Format: port-security mac-address sticky [mac-address <vid>]
Mode:
  • Global Config
  • Interface Config

**Example:** The following shows an example of the command.
(Broadcom FASTPATH)(Config)# port-security mac-address sticky
(Broadcom FASTPATH)(Interface)# port-security mac-address sticky
(Broadcom FASTPATH)(Interface)# port-security mac-address sticky
00:00:00:00:00:01 2

4.33.6.1 no port-security mac-address sticky
The no form removes the sticky mode. The sticky MAC address can be deleted by using the command 'no port-security mac-address <mac-address> <vid>'.

Format: no port-security mac-address sticky [mac-address <vid>]
Mode:
  • Global Config
  • Interface Config

4.33.7 show port-security
This command displays the port-security settings for the port(s). If you do not use a parameter, the command displays the Port Security Administrative mode. Use the optional parameters to display the settings on a specific interface or on all interfaces. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

Format: show port-security [{slot/port | all}]
Mode: Privileged EXEC
For each interface, or for the interface you specify, the following information appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>Port Locking mode for the entire system. This field displays if you do not supply any parameters.</td>
</tr>
<tr>
<td>Dynamic Limit</td>
<td>Maximum dynamically allocated MAC Addresses.</td>
</tr>
<tr>
<td>Static Limit</td>
<td>Maximum statically allocated MAC Addresses.</td>
</tr>
<tr>
<td>Violation Trap Mode</td>
<td>Whether violation traps are enabled.</td>
</tr>
<tr>
<td>Sticky Mode</td>
<td>The administrative mode of the port security Sticky Mode feature on the interface.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show port-security 0/1

<table>
<thead>
<tr>
<th>Intf</th>
<th>Admin Mode</th>
<th>Dynamic Limit</th>
<th>Static Limit</th>
<th>Violation Trap Mode</th>
<th>Sticky Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Disabled</td>
<td>1</td>
<td>1</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### 4.33.8 show port-security dynamic

This command displays the dynamically locked MAC addresses for the port. Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag lag-intf-num` can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number.

**Format**

```
show port-security dynamic slot/port
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>MAC Address of dynamically locked MAC.</td>
</tr>
</tbody>
</table>

### 4.33.9 show port-security static

This command displays the statically locked MAC addresses for port. Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag lag-intf-num` can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number.

**Format**

```
show port-security static {slot/port | lag lag-intf-num}
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statically Configured MAC Address</td>
<td>The statically configured MAC address.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The ID of the VLAN that includes the host with the specified MAC address.</td>
</tr>
<tr>
<td>Sticky</td>
<td>Indicates whether the static MAC address entry is added in sticky mode.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.
(Routing) #show port-security static 0/1

Number of static MAC addresses configured: 2

<table>
<thead>
<tr>
<th>Statically configured MAC Address</th>
<th>VLAN ID</th>
<th>Sticky</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:01</td>
<td>2</td>
<td>Yes</td>
</tr>
<tr>
<td>00:00:00:00:00:02</td>
<td>2</td>
<td>No</td>
</tr>
</tbody>
</table>

4.33.10 show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port. Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag lag-intf-num` can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number.

Format: `show port-security violation {slot/port | lag lag-id}`
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The source MAC address of the last frame that was discarded at a locked port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID, if applicable, associated with the MAC address of the last frame that was discarded at a locked port.</td>
</tr>
</tbody>
</table>

4.34 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.

4.34.1 lldp transmit

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default: disabled
Format: `lldp transmit`
Mode: Interface Config
4.34.1  no lldp transmit
Use this command to return the local data transmission capability to the default.

Format  no lldp transmit
Mode    Interface Config

4.34.2  lldp receive
Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default  disabled
Format    lldp receive
Mode      Interface Config

4.34.2.1  no lldp receive
Use this command to return the reception of LLDPDUs to the default value.

Format    no lldp receive
Mode      Interface Config

4.34.3  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 reinitialization, 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

4.34.3.1  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

4.34.4  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 from an interface or range of interfaces. Use `sys-name` to transmit the system name TLV. To configure the system name, see "snmp-server" on page 71. 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 "description" on page 291.

Default  no optional TLVs are included
Format    lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]
Mode      Interface Config
4.34.4.1 no lldp transmit-tlv
Use this command to remove an optional TLV from the LLDPDU. 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

4.34.5 lldp transmit-mgmt
Use this command to include transmission of the local system management address information in the LLDPDUs. This command can be used to configure a single interface or a range of interfaces.

Format: lldp transmit-mgmt
Mode: Interface Config

4.34.5.1 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

4.34.6 lldp notification
Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default: disabled
Format: lldp notification
Mode: Interface Config

4.34.6.1 no lldp notification
Use this command to disable notifications.

Default: disabled
Format: no lldp notification
Mode: Interface Config

4.34.7 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
4.34.7.1 no lldp notification-interval
Use this command to return the notification interval to the default value.

Format: no lldp notification-interval
Mode: Global Config

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

Format: clear lldp statistics
Mode: Privileged EXEC

4.34.9 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

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

Format: show lldp
Mode: Privileged EXEC

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

4.34.11 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface in a slot/port format.</td>
</tr>
<tr>
<td>Link</td>
<td>Shows whether the link is up or down.</td>
</tr>
<tr>
<td>Transmit</td>
<td>Shows whether the interface transmits LLDPDUs.</td>
</tr>
<tr>
<td>Receive</td>
<td>Shows whether the interface receives LLDPDUs.</td>
</tr>
<tr>
<td>Notify</td>
<td>Shows whether the interface sends remote data change notifications.</td>
</tr>
<tr>
<td>TLVs</td>
<td>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).</td>
</tr>
</tbody>
</table>
4.34.12 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt</td>
<td>Shows whether the interface transmits system management address information in the LLDPDUs.</td>
</tr>
</tbody>
</table>

The table contains the following column headings:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update</td>
<td>The amount of time since the last update to the remote table in days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Total Inserts</td>
<td>Total number of inserts to the remote data table.</td>
</tr>
<tr>
<td>Total Deletes</td>
<td>Total number of deletes from the remote data table.</td>
</tr>
<tr>
<td>Total Drops</td>
<td>Total number of times the complete remote data received was not inserted due to insufficient resources.</td>
</tr>
<tr>
<td>Total Ageouts</td>
<td>Total number of times a complete remote data entry was deleted because the Time to Live interval expired.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface in slot/port format.</td>
</tr>
<tr>
<td>TX Total</td>
<td>Total number of LLDP packets transmitted on the port.</td>
</tr>
<tr>
<td>RX Total</td>
<td>Total number of LLDP packets received on the port.</td>
</tr>
<tr>
<td>Discards</td>
<td>Total number of LLDP frames discarded on the port for any reason.</td>
</tr>
<tr>
<td>Errors</td>
<td>The number of invalid LLDP frames received on the port.</td>
</tr>
<tr>
<td>Ageouts</td>
<td>Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.</td>
</tr>
<tr>
<td>TVL Discards</td>
<td>The number of TLVs discarded.</td>
</tr>
<tr>
<td>TVL Unknowns</td>
<td>Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.</td>
</tr>
<tr>
<td>TLV MED</td>
<td>The total number of LLDP-MED TLVs received on the interface.</td>
</tr>
<tr>
<td>TLV 802.1</td>
<td>The total number of LLDP TLVs received on the interface which are of type 802.1.</td>
</tr>
<tr>
<td>TLV 802.3</td>
<td>The total number of LLDP TLVs received on the interface which are of type 802.3.</td>
</tr>
</tbody>
</table>

4.34.13 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Interface</td>
<td>The interface that received the LLDPDU from the remote device.</td>
</tr>
<tr>
<td>RemID</td>
<td>An internal identifier to the switch to mark each remote device to the system.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(FASTPATH Switching) #show lldp remote-device all

LLDP Remote Device Summary

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>RemID</th>
<th>Chassis ID</th>
<th>Port ID</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/7</td>
<td>2</td>
<td>00:FC:E3:90:01:0F</td>
<td>00:FC:E3:90:01:11</td>
<td></td>
</tr>
<tr>
<td>0/7</td>
<td>3</td>
<td>00:FC:E3:90:01:0F</td>
<td>00:FC:E3:90:01:12</td>
<td></td>
</tr>
<tr>
<td>0/7</td>
<td>4</td>
<td>00:FC:E3:90:01:0F</td>
<td>00:FC:E3:90:01:13</td>
<td></td>
</tr>
<tr>
<td>0/7</td>
<td>5</td>
<td>00:FC:E3:90:01:0F</td>
<td>00:FC:E3:90:01:14</td>
<td></td>
</tr>
<tr>
<td>0/7</td>
<td>1</td>
<td>00:FC:E3:90:01:0F</td>
<td>00:FC:E3:90:03:11</td>
<td></td>
</tr>
<tr>
<td>0/7</td>
<td>6</td>
<td>00:FC:E3:90:01:0F</td>
<td>00:FC:E3:90:04:11</td>
<td></td>
</tr>
<tr>
<td>0/8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

--More-- or (q)uit

4.34.14 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Interface</td>
<td>The interface that received the LLDPDU from the remote device.</td>
</tr>
<tr>
<td>Remote Identifier</td>
<td>An internal identifier to the switch to mark each remote device to the system.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The type of identification used in the Chassis ID field.</td>
</tr>
<tr>
<td>Chassis Subtype</td>
<td>The chassis of the remote device.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>The type of port on the remote device.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port number that transmitted the LLDPDU.</td>
</tr>
<tr>
<td>System Name</td>
<td>The system name of the remote device.</td>
</tr>
<tr>
<td>System Description</td>
<td>Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.</td>
</tr>
<tr>
<td>Port Description</td>
<td>Describes the port in an alpha-numeric format. The port description is configurable.</td>
</tr>
<tr>
<td>System Capabilities Supported</td>
<td>Indicates the primary function(s) of the device.</td>
</tr>
</tbody>
</table>
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

4.34.15 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface in a slot/port format.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port ID associated with this interface.</td>
</tr>
<tr>
<td>Port Description</td>
<td>The port description associated with the interface.</td>
</tr>
</tbody>
</table>

4.34.16 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface that sends the LLDPDU.</td>
</tr>
<tr>
<td>Chassis ID Subtype</td>
<td>The type of identification used in the Chassis ID field.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The chassis of the local device.</td>
</tr>
</tbody>
</table>
4.35 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.

4.35.1 lldp med

Use this command to enable MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default: disabled
Format: lldp med
Mode: Interface Config

4.35.1.1 no lldp med

Use this command to disable MED.

Format: no lldp med
Mode: Interface Config

4.35.2 lldp med confignotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default: disabled
Format: lldp med confignotification
Mode: Interface Config
4.35.2.1 no ldp med confignotification
Use this command to disable notifications.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ldp med confignotification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

4.35.3 ldp 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) from this interface or a range of interfaces.

<table>
<thead>
<tr>
<th>Default</th>
<th>By default, the capabilities and network policy TLVs are included.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>Transmit the LLDP capabilities TLV.</td>
</tr>
<tr>
<td>ex-pd</td>
<td>Transmit the LLDP extended PD TLV.</td>
</tr>
<tr>
<td>ex-pse</td>
<td>Transmit the LLDP extended PSE TLV.</td>
</tr>
<tr>
<td>inventory</td>
<td>Transmit the LLDP inventory TLV.</td>
</tr>
<tr>
<td>location</td>
<td>Transmit the LLDP location TLV.</td>
</tr>
<tr>
<td>network-policy</td>
<td>Transmit the LLDP network policy TLV.</td>
</tr>
</tbody>
</table>

4.35.3.1 no ldp med transmit-tlv
Use this command to remove a TLV.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Format</th>
<th>ldp med all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.35.5 ldp med confignotification all
Use this command to configure all the ports to send the topology change notification.

<table>
<thead>
<tr>
<th>Format</th>
<th>ldp med confignotification all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>
4.35.6  lldp med faststartrepeatcount
Use this command to set the value of the fast start repeat count. \([\text{count}]\) 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

4.35.6.1  no lldp med faststartrepeatcount
Use this command to return to the factory default value.

**Format** `no lldp med faststartrepeatcount`

**Mode** Global Config

4.35.7  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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>Transmit the LLDP capabilities TLV.</td>
</tr>
<tr>
<td>ex-pd</td>
<td>Transmit the LLDP extended PD TLV.</td>
</tr>
<tr>
<td>ex-pse</td>
<td>Transmit the LLDP extended PSE TLV.</td>
</tr>
<tr>
<td>inventory</td>
<td>Transmit the LLDP inventory TLV.</td>
</tr>
<tr>
<td>location</td>
<td>Transmit the LLDP location TLV.</td>
</tr>
<tr>
<td>network-policy</td>
<td>Transmit the LLDP network policy TLV.</td>
</tr>
</tbody>
</table>

4.35.7.1  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

4.35.8  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.

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

Fast Start Repeat Count: 3
Device Class: Network Connectivity

(FASTPATH Routing) #

4.35.9  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.

(FASTPATH Routing) #show lldp med interface all

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>configMED</th>
<th>operMED</th>
<th>ConfigNotify</th>
<th>TLVsTx</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/2</td>
<td>Up</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/3</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/4</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/5</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/6</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/7</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/8</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/9</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/10</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/11</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/12</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/13</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>0/14</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
</tbody>
</table>

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

--More-- or (q)uit

(FASTPATH Routing) #show lldp med interface 0/2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>configMED</th>
<th>operMED</th>
<th>ConfigNotify</th>
<th>TLVsTx</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/2</td>
<td>Up</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #
4.35.10 show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits.  \textit{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.

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

LLDP MED Local Device Detail

Interface: 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
4.35.11  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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Interface</td>
<td>The interface that received the LLDPDU from the remote device.</td>
</tr>
<tr>
<td>Remote ID</td>
<td>An internal identifier to the switch to mark each remote device to the system.</td>
</tr>
<tr>
<td>Device Class</td>
<td>Device classification of the remote device.</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the command. (FASTPATH Routing) #show lldp med remote-device all

LLDP MED Remote Device Summary

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>Remote ID</th>
<th>Device Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/8</td>
<td>1</td>
<td>Class I</td>
</tr>
<tr>
<td>0/9</td>
<td>2</td>
<td>Not Defined</td>
</tr>
<tr>
<td>0/10</td>
<td>3</td>
<td>Class II</td>
</tr>
<tr>
<td>0/11</td>
<td>4</td>
<td>Class III</td>
</tr>
<tr>
<td>0/12</td>
<td>5</td>
<td>Network Con</td>
</tr>
</tbody>
</table>

4.35.12  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. (FASTPATH Routing) #show lldp med remote-device detail 0/8

LLDP MED Remote Device Detail

Local Interface: 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
4.36 Denial of Service Commands

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

This section describes the commands you use to configure Denial of Service (DoS) Control. FASTPATH software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- SIP = DIP: Source IP address = Destination IP address.
- First Fragment: TCP Header size smaller then configured value.
- TCP Fragment: Allows the device to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
- 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.
- SMAC = DMAC: Source MAC address = Destination MAC address
- TCP Port: Source TCP Port = Destination TCP Port
- UDP Port: Source UDP Port = Destination UDP Port
- TCP Flag & Sequence: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- TCP Offset: Allows the device to drop packets that have a TCP header Offset set to 1.
- TCP SYN: TCP Flag SYN set.
- TCP SYN & FIN: TCP Flags SYN and FIN set.
- TCP FIN & URG & PSH: TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- ICMP V6: Limiting the size of ICMPv6 Ping packets.
- ICMP Fragment: Checks for fragmented ICMP packets.

4.36.1 dos-control all

This command enables Denial of Service protection checks globally.

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

Monitoring and blocking of the types of attacks listed below are only supported on the BCM56224, BCM56514, BCM56624, BCM56634, BCM56636 and BCM56820 platforms.
4.36.1  no dos-control all
This command disables Denial of Service prevention checks globally.

**Format**
no dos-control all

**Mode**
Global Config

4.36.2  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

4.36.2.1  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

4.36.3  dos-control firstfrag
This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled. The default is disabled. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to 20.

**Default**
disabled (20)

**Format**
dos-control firstfrag [0-255]

**Mode**
Global Config

4.36.3.1  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

4.36.4  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 and packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size are dropped.

**Default**
disabled

**Format**
dos-control tcpfrag

**Mode**
Global Config
4.36.4.1  no dos-control tcpfrag
This command disables TCP Fragment Denial of Service protection.

Format: no dos-control tcpfrag
Mode: Global Config

4.36.5  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

4.36.5.1  no dos-control tcpflag
This command sets disables TCP Flag Denial of Service protections.

Format: no dos-control tcpflag
Mode: Global Config

4.36.6  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.

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
4.36.6.1  no dos-control l4port
This command disables L4 Port Denial of Service protections.

<table>
<thead>
<tr>
<th>Format</th>
<th>no dos-control l4port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.36.7  dos-control smacdmac

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

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>dos-control smacdmac</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.36.7.1  no dos-control smacdmac
This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

<table>
<thead>
<tr>
<th>Format</th>
<th>no dos-control smacdmac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

4.36.8  dos-control tcpport

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

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>dos-control tcpport</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>
4.36.8.1 no dos-control tcpport
This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format no dos-control tcpport
Mode Global Config

4.36.9 dos-control udpport

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

Default disabled
Format dos-control udpport
Mode Global Config

4.36.9.1 no dos-control udpport
This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format no dos-control udpport
Mode Global Config

4.36.10 dos-control tcpflagseq

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default disabled
Format dos-control tcpflagseq
Mode Global Config
4.36.10.1 no dos-control tcpflagseq
This command sets disables TCP Flag and Sequence Denial of Service protection.

**Format**
no dos-control tcpflagseq

**Mode**
Global Config

4.36.11 dos-control tcpoffset

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

**Default**
disabled

**Format**
dos-control tcpoffset

**Mode**
Global Config

4.36.11.1 no dos-control tcpoffset
This command disabled TCP Offset Denial of Service protection.

**Format**
no dos-control tcpoffset

**Mode**
Global Config

4.36.12 dos-control tcpsyn

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

**Default**
disabled

**Format**
dos-control tcpsyn

**Mode**
Global Config
4.36.12 no dos-control tcpsyn
This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format: no dos-control tcpsyn
Mode: Global Config

4.36.13 dos-control tcpsynfin

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

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

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

4.36.13.1 no dos-control tcpsynfin
This command sets disables TCP SYN & FIN Denial of Service protection.

Format: no dos-control tcpsynfin
Mode: Global Config

4.36.14 dos-control tcpfinurgpsh

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

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

Default: disabled
Format: dos-control tcpfinurgpsh
Mode: Global Config
4.36.14.1 no dos-control tcpfinurgpsh
This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format: no dos-control tcpfinurgpsh
Mode: Global Config

4.36.15 dos-control icmpv4

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default: disabled (512)
Format: dos-control icmpv4 [0-16376]
Mode: Global Config

4.36.15.1 no dos-control icmpv4
This command disables Maximum ICMP Packet Size Denial of Service protections.

Format: no dos-control icmpv4
Mode: Global Config

4.36.16 dos-control icmpv6

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default: disabled (512)
Format: dos-control icmpv6 [0-16376]
Mode: Global Config
4.36.16.1  no dos-control icmpv6
This command disables Maximum ICMP Packet Size Denial of Service protections.

Format  no dos-control icmpv6  
Mode    Global Config

4.36.17  dos-control icmpfrag

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default  disabled  
Format    dos-control icmpfrag  
Mode    Global Config

4.36.17.1  no dos-control icmpfrag
This command disabled ICMP Fragment Denial of Service protection.

Format    no dos-control icmpfrag  
Mode    Global Config

4.36.18  show dos-control
This command displays Denial of Service configuration information.

Format    show dos-control  
Mode    Privileged EXEC

---

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Fragment Mode</td>
<td>The administrative mode of First Fragment DoS prevention. When enabled, this causes the switch to drop packets that have a TCP header smaller than the configured Min TCP Hdr Size.</td>
</tr>
<tr>
<td>Min TCP Hdr Size</td>
<td>The minimum TCP header size the switch will accept if First Fragment DoS prevention is enabled.</td>
</tr>
<tr>
<td>ICMPv4 Mode</td>
<td>The administrative mode of ICMPv4 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 Payload Size.</td>
</tr>
<tr>
<td>Max ICMPv4 Payload Size</td>
<td>The maximum ICMPv4 payload size to accept when ICMPv4 DoS protection is enabled.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ICMPv6 Mode</td>
<td>The administrative mode of ICMPv6 DoS prevention. When enabled, this causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Payload Size.</td>
</tr>
<tr>
<td>Max ICMPv6 Payload Size</td>
<td>The maximum ICMPv6 payload size to accept when ICMPv6 DoS protection is enabled.</td>
</tr>
<tr>
<td>ICMPv4 Fragment Mode</td>
<td>The administrative mode of ICMPv4 Fragment DoS prevention. When enabled, this causes the switch to drop fragmented ICMPv4 packets.</td>
</tr>
<tr>
<td>TCP Port Mode</td>
<td>The administrative mode of TCP Port DoS prevention. When enabled, this causes the switch to drop packets that have the TCP source port equal to the TCP destination port.</td>
</tr>
<tr>
<td>UDP Port Mode</td>
<td>The administrative mode of UDP Port DoS prevention. When enabled, this causes the switch to drop packets that have the UDP source port equal to the UDP destination port.</td>
</tr>
<tr>
<td>SIPDIP Mode</td>
<td>The administrative mode of SIP=DIP DoS prevention. Enabling this causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.</td>
</tr>
<tr>
<td>SMACDMAC Mode</td>
<td>The administrative mode of SMAC=DMAC DoS prevention. Enabling this causes the switch to drop packets that have a source MAC address equal to the destination MAC address.</td>
</tr>
<tr>
<td>TCP FIN&amp;URG&amp; PSH Mode</td>
<td>The administrative mode of TCP FIN &amp; URG &amp; PSH DoS prevention. Enabling this causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0.</td>
</tr>
<tr>
<td>TCP Flag &amp; Sequence Mode</td>
<td>The administrative mode of TCP Flag DoS prevention. Enabling this causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0.</td>
</tr>
<tr>
<td>TCP SYN Mode</td>
<td>The administrative mode of TCP SYN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN set.</td>
</tr>
<tr>
<td>TCP SYN &amp; FIN Mode</td>
<td>The administrative mode of TCP SYN &amp; FIN DoS prevention. Enabling this causes the switch to drop packets that have TCP Flags SYN and FIN set.</td>
</tr>
<tr>
<td>TCP Fragment Mode</td>
<td>The administrative mode of TCP Fragment DoS prevention. Enabling this causes the switch to drop packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size.</td>
</tr>
<tr>
<td>TCP Offset Mode</td>
<td>The administrative mode of TCP Offset DoS prevention. Enabling this causes the switch to drop packets that have a TCP header Offset equal to 1.</td>
</tr>
</tbody>
</table>
4.37 MAC Database Commands

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

4.37.1 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. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

| Default | 300 |
| Format  | bridge aging-time 10-1,000,000 |
| Mode    | Global Config |

4.37.1.1 no bridge aging-time

This command sets the forwarding database address aging timeout to the default value. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

| Format  | no bridge aging-time |
| Mode    | Global Config |

4.37.2 show forwardingdb agetime

This command displays the timeout for address aging.

| Default | all |
| Format  | show forwardingdb agetime |
| Mode    | Privileged EXEC |

4.37.3 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 |

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Aging Timeout</td>
<td>Displays the system's address aging timeout value in seconds.</td>
</tr>
</tbody>
</table>

4.37.3.1 show mac-address-table multicast macaddr

| Format  | show mac-address-table multicast macaddr |
| Mode    | Privileged EXEC |

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN in which the MAC address is learned.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.</td>
</tr>
<tr>
<td>Source</td>
<td>The component that is responsible for this entry in the Multicast Forwarding Database. The source can be IGMP Snooping, GMRP, and Static Filtering.</td>
</tr>
<tr>
<td>Type</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of this multicast table entry.</td>
</tr>
</tbody>
</table>
Example: If one or more entries exist in the multicast forwarding table, the command output looks similar to the following:

(Routing) #show mac-address-table multicast

--- More --- or (q)uit

4.37.4  show mac-address-table stats

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

Format  show mac-address-table stats
Mode    Privileged EXEC

4.38  ISDP Commands

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

4.38.1  isdp run

This command enables ISDP on the switch.

Default  Enabled
Format    isdp run
Mode      Global Config
4.38.1 no isdp run
This command disables ISDP on the switch.

**Format**  
no isdp run

**Mode**  
Global Config

4.38.2 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

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

**Default**  
60 seconds

**Format**  
isdp timer 5-254

**Mode**  
Global Config

4.38.4 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

4.38.4.1 no isdp advertise-v2
This command disables the sending of ISDP version 2 packets from the device.

**Format**  
o no isdp advertise-v2

**Mode**  
Global Config

4.38.5 isdp enable
This command enables ISDP on an interface or range of interfaces.

---

**NOTICE**

ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command “isdp run” on page 499.

**Default**  
Enabled

**Format**  
isdp enable

**Mode**  
Interface Config
4.38.5.1  no isdp enable
This command disables ISDP on the interface.

Format  no isdp enable
Mode    Interface Config

4.38.6  clear isdp counters
This command clears ISDP counters.

Format  clear isdp counters
Mode    Privileged EXEC

4.38.7  clear isdp table
This command clears entries in the ISDP table.

Format  clear isdp table
Mode    Privileged EXEC

4.38.8  show isdp
This command displays global ISDP settings.

Format  show isdp
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer</td>
<td>The frequency with which this device sends ISDP packets. This value is given in seconds.</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The length of time the receiving device should save information sent by this device. This value is given in seconds.</td>
</tr>
<tr>
<td>Version 2 Advertisements</td>
<td>The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.</td>
</tr>
<tr>
<td>Neighbors table time since last change</td>
<td>The amount of time that has passed since the ISPD neighbor table changed.</td>
</tr>
<tr>
<td>Device ID</td>
<td>The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.</td>
</tr>
<tr>
<td>Device ID Format Capability</td>
<td>Indicates the Device ID format capability of the device.</td>
</tr>
<tr>
<td></td>
<td>•  serialNumber indicates that the device uses a serial number as the format for its Device ID.</td>
</tr>
<tr>
<td></td>
<td>•  macAddress indicates that the device uses a Layer 2 MAC address as the format for its Device ID.</td>
</tr>
<tr>
<td></td>
<td>•  other indicates that the device uses its platform-specific format as the format for its Device ID.</td>
</tr>
<tr>
<td>Device ID Format</td>
<td>Indicates the Device ID format of the device.</td>
</tr>
<tr>
<td></td>
<td>•  serialNumber indicates that the value is in the form of an ASCII string containing the device serial number.</td>
</tr>
<tr>
<td></td>
<td>•  macAddress indicates that the value is in the form of a Layer 2 MAC address.</td>
</tr>
<tr>
<td></td>
<td>•  other indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepend-ed with system name.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

```plaintext
(FASTPATH Routing) #show isdp

Timer........................................... 30
Hold Time...................................... 180
Version 2 Advertisements..................... Enabled
Neighbors table time since last change....... 0 days 00:00:00
Device ID........................................ 1114728
Device ID format capability.................... Serial Number, Host Name
Device ID format............................... Serial Number
```

### 4.38.9 show isdp interface

This command displays ISDP settings for the specified interface.

**Format**

```
show isdp interface {all | slot/port}
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The slot/port of the specified interface.</td>
</tr>
<tr>
<td>Mode</td>
<td>ISDP mode enabled/disabled status for the interface(s).</td>
</tr>
</tbody>
</table>

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

```plaintext
(Routing) #show isdp interface 0/1

Interface Mode
------------- -------
0/1           Enabled
```

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

```plaintext
(Switching) #show isdp interface all

Interface Mode
------------- -------
0/1           Enabled
0/2           Enabled
0/3           Enabled
0/4           Enabled
0/5           Enabled
0/6           Enabled
0/7           Enabled
0/8           Enabled
```
4.38.10  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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>The device ID associated with the neighbor which advertised the information.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>The IP address(es) associated with the neighbor.</td>
</tr>
<tr>
<td>Capability</td>
<td>ISDP Functional Capabilities advertised by the neighbor.</td>
</tr>
<tr>
<td>Platform</td>
<td>The hardware platform advertised by the neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface (slot/port) on which the neighbor's advertisement was received.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port ID of the interface from which the neighbor sent the advertisement.</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The hold time advertised by the neighbor.</td>
</tr>
<tr>
<td>Version</td>
<td>The software version that the neighbor is running.</td>
</tr>
<tr>
<td>Advertisement Version</td>
<td>The version of the advertisement packet received from the neighbor.</td>
</tr>
<tr>
<td>Entry Last Changed Time</td>
<td>The time when the entry was last changed.</td>
</tr>
</tbody>
</table>

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

(Switching) #show isdp entry Switch

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address(es):</td>
<td>172.20.1.18</td>
</tr>
<tr>
<td>IP Address:</td>
<td>172.20.1.18</td>
</tr>
<tr>
<td>Capability</td>
<td>Router IGMP</td>
</tr>
<tr>
<td>Platform</td>
<td>cisco WS-C4948</td>
</tr>
<tr>
<td>Interface</td>
<td>0/1</td>
</tr>
<tr>
<td>Port ID</td>
<td>GigabitEthernet1/1</td>
</tr>
<tr>
<td>Holdtime</td>
<td>64</td>
</tr>
<tr>
<td>Advertisement Version</td>
<td>2</td>
</tr>
<tr>
<td>Entry last changed time</td>
<td>0 days 00:13:50</td>
</tr>
</tbody>
</table>

4.38.11  show isdp neighbors

This command displays the list of neighboring devices.

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

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>The device ID associated with the neighbor which advertised the information.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>The IP addresses associated with the neighbor.</td>
</tr>
<tr>
<td>Capability</td>
<td>ISDP functional capabilities advertised by the neighbor.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.
(Switching) #show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Intf</th>
<th>Holdtime</th>
<th>Capability</th>
<th>Platform</th>
<th>Port ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>0/1</td>
<td>165</td>
<td>RI</td>
<td>cisco WS-C4948</td>
<td>GigabitEthernet1/1</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the command.
(Switching) #show isdp neighbors detail

Device ID          0001f45f1bc0
Address(es):       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

4.38.12 show isdp traffic
This command displays ISDP statistics.

Format: show isdp traffic
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDP Packets Received</td>
<td>Total number of ISDP packets received</td>
</tr>
<tr>
<td>ISDP Packets Transmitted</td>
<td>Total number of ISDP packets transmitted</td>
</tr>
<tr>
<td>ISDPv1 Packets Received</td>
<td>Total number of ISDPv1 packets received</td>
</tr>
<tr>
<td>ISDPv1 Packets Transmitted</td>
<td>Total number of ISDPv1 packets transmitted</td>
</tr>
<tr>
<td>ISDPv2 Packets Received</td>
<td>Total number of ISDPv2 packets received</td>
</tr>
<tr>
<td>ISDPv2 Packets Transmitted</td>
<td>Total number of ISDPv2 packets transmitted</td>
</tr>
<tr>
<td>ISDP Bad Header</td>
<td>Number of packets received with a bad header</td>
</tr>
<tr>
<td>ISDP Checksum Error</td>
<td>Number of packets received with a checksum error</td>
</tr>
<tr>
<td>ISDP Transmission Failure</td>
<td>Number of packets which failed to transmit</td>
</tr>
<tr>
<td>ISDP Invalid Format</td>
<td>Number of invalid packets received</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(FASTPATH Routing) #show isdp traffic

| ISDP Table Full | Number of times a neighbor entry was not added to the table due to a full database |
| ISDP IP Address Table Full | Displays the number of times a neighbor entry was added to the table without an IP address. |

Example:

(FASTPATH Routing) #show isdp traffic

| ISDP Packets Received | 4253 |
| ISDP Packets Transmitted | 127 |
| ISDPv1 Packets Received | 0 |
| ISDPv1 Packets Transmitted | 0 |
| ISDPv2 Packets Received | 4253 |
| ISDPv2 Packets Transmitted | 4351 |
| ISDP Bad Header | 0 |
| ISDP Checksum Error | 0 |
| ISDP Transmission Failure | 0 |
| ISDP Invalid Format | 0 |
| ISDP Table Full | 392 |
| ISDP IP Address Table Full | 737 |

4.38.13 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

4.38.13.1 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

4.39 Interface Error Disable and Auto Recovery

Interface error disable automatically disables an interface when an error is detected; no traffic is allowed until the interface is either manually re-enabled or, if auto recovery is configured, the configured auto recovery time interval has passed.

For interface error disable and auto recovery, an error condition is detected for an interface, the interface is placed in a diagnostic disabled state by shutting down the interface. The error disabled interface does not allow any traffic until the interface is re-enabled. The error disabled interface can be manually enabled. Alternatively administrator can enable auto recovery feature. FASTPATH Auto Recovery re-enables the interface after the expiry of configured time interval.
4.39.1 errdisable recovery cause

Use this command to enable auto recovery for a specified cause or all causes. When auto recovery is enabled, ports in the diag-disable state are recovered (link up) when the recovery interval expires. If the interface continues to experience errors, the interface may be placed back in the diag-disable state and disabled (link down). Interfaces in the diag-disable state can be manually recovered by entering the no shutdown command for the interface.

Default: None

Format: errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp-mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service | link-flap}

Mode: Global Config

4.39.1.1 no errdisable recovery cause

Use this command to disable auto recovery for a specific cause. When disabled, auto recovery will not occur for interfaces in a diag-disable state due to that cause.

Format: no errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp-mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service | link-flap}

Mode: Global Config

4.39.2 errdisable recovery interval

Use this command to configure the auto recovery time interval. The auto recovery time interval is common for all causes. The time can be any value from 30 to 86400 seconds. When the recovery interval expires, the system attempts to bring interfaces in the diag-disable state back into service (link up).

Default: 300

Format: errdisable recovery interval 30-86400

Mode: Global Config

4.39.2.1 no errdisable recovery interval

Use this command to reset the auto recovery interval to the factory default value of 300.

Format: no errdisable recovery interval

Mode: Global Config

4.39.3 show errdisable recovery

Use this command to display the errdisable configuration status of all configurable causes.

Format: show errdisable recovery

Mode: Privileged EXEC

The following information is displayed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-rate-limit</td>
<td>Enable/Disable status of dhcp-rate-limit auto recovery.</td>
</tr>
<tr>
<td>arp-inspection</td>
<td>Enable/Disable status of arp-inspection auto recovery.</td>
</tr>
<tr>
<td>sfp-mismatch</td>
<td>Enable/Disable status of sfp-mismatch auto recovery.</td>
</tr>
<tr>
<td>udld</td>
<td>Enable/Disable status of UDLD auto recovery.</td>
</tr>
</tbody>
</table>
### Example:
Errdisable Reason | Auto-recovery Status
-----------------|---------------------
dhcp-rate-limit   | Disabled            
ar-p-inspection   | Disabled            
udld              | Disabled            
bcast-storm       | Disabled            
mcast-storm       | Disabled            
ucast-storm       | Disabled            
bpduguard         | Disabled            
bpdustorm         | Disabled            
sfp-mismatch      | Disabled            
keepalive         | Disabled            
mac-locking       | Disabled            
denial-of-service| Disabled            
link-flap          | Disabled            

Timeout for Auto-recovery from D-Disable state 300

4.39.4  **show interfaces status err-disabled**

Use this command to display the interfaces that are error disabled and the amount of time remaining for auto recovery.

**Format**  
show interfaces status err-disabled

**Mode**  
Privileged EXEC
The following information is displayed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>An interface that is error disabled.</td>
</tr>
<tr>
<td>Errdisable Reason</td>
<td>The cause of the interface being error disabled.</td>
</tr>
<tr>
<td>Auto-Recovery</td>
<td>The amount of time left before auto recovery begins.</td>
</tr>
<tr>
<td>Time Left</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

(Routing) #show interfaces status err-disabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>Errdisable Reason</th>
<th>Auto-Recovery Time Left(sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>udld</td>
<td>279</td>
</tr>
<tr>
<td>0/2</td>
<td>bpduguard</td>
<td>285</td>
</tr>
<tr>
<td>0/3</td>
<td>bpdustorm</td>
<td>291</td>
</tr>
<tr>
<td>0/4</td>
<td>keepalive</td>
<td>11</td>
</tr>
</tbody>
</table>

### 4.40 Port Bridging Commands

#### 4.40.1 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

#### 4.40.1.1 no L2-port-bridge

This command resets L2 port bridging.

**Format**

```
no L2-port-bridge
```

**Mode**

Interface Config

#### 4.40.2 show port L2-port-bridge

This command displays the L2 port bridge setting. The command displays for a specified interface or all interfaces the settings. The displayed fields are

- the interface
- enabled/disabled L2 port bridge

**Format**

```
show port L2-port-bridge {<unit/slot/port> | all}
```

**Mode**

Privileged Exec
5 / Routing Commands

This chapter describes the routing commands available in the FASTPATH CLI.
The Routing Commands chapter contains the following sections:
• “Address Resolution Protocol Commands” on page 509
• “IP Routing Commands” on page 514
• “Routing Policy Commands” on page 535
• “Router Discovery Protocol Commands” on page 549
• “Virtual Router Redundancy Protocol Commands” on page 555
• “VRRPv3 Commands” on page 562
• “DHCP and BOOTP Relay Commands” on page 573
• “IP Helper Commands” on page 577
• “Open Shortest Path First Commands” on page 583
• “Routing Information Protocol Commands” on page 631
• “ICMP Throttling Commands” on page 638
• “Bidirectional Forwarding Detection Commands” on page 640

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 Address Resolution Protocol Commands

This section describes the commands you use to configure Address Resolution Protocol (ARP) and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

5.1.1 arp

This command creates an ARP entry. The value for ipaddress is the IP address of a device on a subnet attached to an existing routing interface. The parameter macaddr is a unicast MAC address for that device. The interface parameter specifies the next hop interface.

The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format      arp ipaddress macaddr interface {unit/slot/port | vlan id}
Mode        Global Config
5.1.1 no arp

This command deletes an ARP entry. The value for *arpentry* is the IP address of the interface. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device. The interface parameter specifies the next hop interface.

**Format**
```
no arp ipaddress macaddr interface unit/slot/port
```

**Mode**
Global Config

5.1.2 ip proxy-arp

This command enables proxy ARP on a router interface or range of interfaces. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

**Default**
enabled

**Format**
```
ip proxy-arp
```

**Mode**
Interface Config

5.1.2.1 no ip proxy-arp

This command disables proxy ARP on a router interface.

**Format**
```
no ip proxy-arp
```

**Mode**
Interface Config

5.1.3 ip local-proxy-arp

Use this command to allow an interface to respond to ARP requests for IP addresses within the subnet and to forward traffic between hosts in the subnet.

**Default**
.disabled

**Format**
```
ip local-proxy-arp
```

**Mode**
Interface Config

5.1.3.1 no ip local-proxy-arp

This command resets the local proxy ARP mode on the interface to the default value.

**Format**
```
no ip local-proxy-arp
```

**Mode**
Interface Config
5.1.4  arp cachesize
This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

Format  
Mode  Global Config

5.1.4.1 no arp cachesize
This command configures the default ARP cache size.

Format  
Mode  Global Config

5.1.5  arp dynamicrenew
This command enables the ARP component to automatically renew dynamic ARP entries when they age out. When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host may be lost until the router receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option applies only to host entries.
The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Default  
Format  
Mode  Privileged EXEC

5.1.5.1 no arp dynamicrenew
This command prevents dynamic ARP entries from renewing when they age out.

Format  
Mode  Privileged EXEC

5.1.6  arp purge
This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format  
Mode  Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>The IP address to remove from the ARP cache.</td>
</tr>
<tr>
<td>interface</td>
<td>The interface from which IP addresses will be removed.</td>
</tr>
</tbody>
</table>
5.1.7  

arp resptime  
This command configures the ARP request response timeout.  
The value for `seconds` is a valid positive integer, which represents the IP ARP entry response timeout time in seconds.  
The range for `seconds` is between 1-10 seconds.  

Default 1  
Format `arp resptime 1-10`  
Mode Global Config  

5.1.7.1 no arp resptime  
This command configures the default ARP request response timeout.  

Format `no arp resptime`  
Mode Global Config  

5.1.8  

arp retries  
This command configures the ARP count of maximum request for retries.  
The value for `retries` is an integer, which represents the maximum number of request for retries. The range for `retries` is an integer between 0-10 retries.  

Default 4  
Format `arp retries 0-10`  
Mode Global Config  

5.1.8.1 no arp retries  
This command configures the default ARP count of maximum request for retries.  

Format `no arp retries`  
Mode Global Config  

5.1.9  

arp timeout  
This command configures the ARP entry ageout time.  
The value for `seconds` is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for `seconds` is between 15-21600 seconds.  

Default 1200  
Format `arp timeout 15-21600`  
Mode Global Config
5.1.9.1  no arp timeout
This command configures the default ARP entry ageout time.

Format  no arp timeout
Mode     Global Config

5.1.10  clear arp-cache
This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the gateway keyword is specified, the dynamic entries of type gateway are purged as well.

Format  clear arp-cache [gateway]
Mode     Privileged EXEC

5.1.11  clear arp-switch
Use this command to clear the contents of the switch’s Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, ping from the remote system to the DUT. Issue the show arp switch command to see the ARP entries. Then issue the clear arp-switch command and check the show arp switch entries. There will be no more arp entries.

Format  clear arp-switch
Mode     Privileged EXEC

5.1.12  show arp
This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the show arp results in conjunction with the show arp switch results.

Format  show arp
Mode     Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age Time (seconds)</td>
<td>The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.</td>
</tr>
<tr>
<td>Response Time (seconds)</td>
<td>The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.</td>
</tr>
<tr>
<td>Retries</td>
<td>The maximum number of times an ARP request is retried. This value is configurable.</td>
</tr>
<tr>
<td>Cache Size</td>
<td>The maximum number of entries in the ARP table. This value is configurable.</td>
</tr>
<tr>
<td>Dynamic Renew Mode</td>
<td>Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.</td>
</tr>
<tr>
<td>Total Entry Count Current / Peak</td>
<td>The total entries in the ARP table and the peak entry count in the ARP table.</td>
</tr>
<tr>
<td>Static Entry Count Current / Max</td>
<td>The static entry count in the ARP table and maximum static entry count in the ARP table.</td>
</tr>
</tbody>
</table>

The following are displayed for each ARP entry:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of a device on a subnet attached to an existing routing interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The hardware MAC address of that device.</td>
</tr>
</tbody>
</table>
5.1.13  **show arp brief**

This command displays the brief Address Resolution Protocol (ARP) table information.

<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The routing <code>slot/port</code> associated with the device ARP entry.</td>
</tr>
<tr>
<td>Type</td>
<td>The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.</td>
</tr>
<tr>
<td>Age</td>
<td>The current age of the ARP entry since last refresh (in hh:mm:ss format)</td>
</tr>
</tbody>
</table>

**Format**  
`show arp brief`

**Mode**  
Privileged EXEC

5.1.14  **show arp switch**

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The routing <code>slot/port</code> associated with the device's ARP entry.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of a device on a subnet attached to the switch.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The hardware MAC address of that device.</td>
</tr>
</tbody>
</table>

**Format**  
`show arp switch`

**Mode**  
Privileged EXEC

5.2  **IP Routing Commands**

This section describes the commands you use to enable and configure IP routing on the switch.

5.2.1  **routing**

This command enables IPv4 and IPv6 routing for an interface or range of interfaces. You can view the current value for this function with the `show ip brief` command. The value is labeled as “Routing Mode.”

<table>
<thead>
<tr>
<th><strong>Default</strong></th>
<th><code>disabled</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Format</strong></td>
<td><code>routing</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Config</td>
</tr>
</tbody>
</table>
5.2.1 no routing
This command disables routing for an interface.
You can view the current value for this function with the `show ip brief` command. The value is labeled as "Routing Mode."

```
Format          no routing
Mode            Interface Config
```

5.2.2 ip routing
This command enables the IP Router Admin Mode for the master switch.

```
Format          ip routing
Mode            • Global Config
                • Virtual Router Config
```

5.2.2.1 no ip routing
This command disables the IP Router Admin Mode for the master switch.

```
Format          no ip routing
Mode            Global Config
```

5.2.3 ip address
This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface. The command supports RFC 3021 and accepts using 31-bit prefixes on IPv4 point-to-point links. This command adds the label IP address in the command "show ip interface" on page 523.

### NOTICE
The 31-bit subnet mask is only supported on routing interfaces. The feature is not supported on network port and service port interfaces because FASTPATH acts as a host, not a router, on these management interfaces.

```
Format          ip address ipaddr {subnetmask | /masklen} [secondary]
Mode            Interface Config
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td>subnetmask</td>
<td>A 4-digit dotted-decimal number which represents the subnet mask of the interface.</td>
</tr>
<tr>
<td>masklen</td>
<td>Implements RFC 3021. Using the / notation of the subnet mask, this is an integer that indicates the length of the subnet mask. Range is 5 to 32 bits.</td>
</tr>
</tbody>
</table>

**Example:** The following example of the command shows the configuration of the subnet mask with an IP address in the dotted decimal format on interface 0/4/1.

```
(router1) #config
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address 192.168.10.1 255.255.255.254
```
**Example:** The next example of the command shows the configuration of the subnet mask with an IP address in the / notation on interface 0/4/1.

```
(router1) #config
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address 192.168.10.1 /31
```

### 5.2.3.1 no ip address

This command deletes an IP address from an interface. The value for `ipaddr` is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for `subnetmask` is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command `no ip address`.

**Format**
```
no ip address [{ipaddr subnetmask [secondary]}]
```

**Mode**
Interface Config

### 5.2.4 ip address dhcp

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

To enable the DHCPv4 client on an in-band interface and send DHCP client messages with the client identifier option, use the `ip address dhcp client-id` configuration command in interface configuration mode.

**Default**
disabled

**Format**
```
ip address dhcp [client-id]
```

**Mode**
Interface Config

**Example:** In the following example, DHCPv4 is enabled on interface 0/4/1.

```
(router1) #config
(router1) (Config)#interface 0/4/1
(router1) (Interface 0/4/1)#ip address dhcp
```

### 5.2.4.1 no ip address dhcp

The `no ip address dhcp` command releases a leased address and disables DHCPv4 on an interface. The no form of the `ip address dhcp client-id` command removes the client-id option and also disables the DHCP client on the in-band interface.

**Format**
```
no ip address dhcp [client-id]
```

**Mode**
Interface Config

### 5.2.5 ip default-gateway

This command manually configures a default gateway for the switch. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway. The system installs a default IPv4 route with the gateway address as the next hop address. The route preference is 253. A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server.

**Format**
```
ip default-gateway ipaddr
```

**Mode**

- Global Config
Example: The following example sets the default gateway to 10.1.1.1.
(router1) #config
(router1) (Config)#ip default-gateway 10.1.1.1

5.2.5.1 no ip default-gateway
This command removes the default gateway address from the configuration.

Format no ip default-gateway ipaddr
Mode Interface Config

5.2.6 ip load-sharing
This command configures IP ECMP load balancing mode.

Default 6
Format ip load-sharing mode {inner | outer}
Mode Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode</td>
<td>Configures the load balancing or sharing mode for all EMCP groups.</td>
</tr>
<tr>
<td></td>
<td>• 1: Based on a hash using the Source IP address of the packet.</td>
</tr>
<tr>
<td></td>
<td>• 2: Based on a hash using the Destination IP address of the packet.</td>
</tr>
<tr>
<td></td>
<td>• 3: Based on a hash using the Source and Destination IP addresses of the packet.</td>
</tr>
<tr>
<td></td>
<td>• 4: Based on a hash using the Source IP address and the Source TCP/UDP Port field of the packet.</td>
</tr>
<tr>
<td></td>
<td>• 5: Based on a hash using the Destination IP address and the Destination TCP/UDP Port field of the packet.</td>
</tr>
<tr>
<td></td>
<td>• 6: Based on a hash using the Source and Destination IP address, and the Source and Destination TCP/UDP Port fields of the packet.</td>
</tr>
<tr>
<td>inner</td>
<td>Use the inner IP header for tunneled packets.</td>
</tr>
<tr>
<td>outer</td>
<td>Use the outer IP header for tunneled packets.</td>
</tr>
</tbody>
</table>

5.2.6.1 no ip load-sharing

Format no ip load-sharing
Mode Global Config

5.2.7 release dhcp
Use this command to force the DHCPv4 client to release the leased address from the specified interface. The DHCP client sends a DHCP Release message telling the DHCP server that it no longer needs the IP address, and that the IP address can be reassigned to another
5.2.8 renew dhc

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

This command can be used on in-band ports as well as the service or network (out-of-band) port.

Format: renew dhcp slot/port
Mode: Privileged EXEC

5.2.9 renew dhcp network-port

Use this command to renew an IP address on a network port.

Format: renew dhcp network-port
Mode: Privileged EXEC

5.2.10 renew dhcp service-port

Use this command to renew an IP address on a service port.

Format: renew dhcp service-port
Mode: Privileged EXEC

5.2.11 ip route

This command configures a static route. The ipaddr parameter is a valid IP address, and subnetmask is a valid subnet mask. The nexthopip parameter is a valid IP address of the next hop router. Specifying Null0 as nexthop parameter adds a static reject route. The optional preference parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Default: preference—1

Format: ip route ipaddr subnetmask { slot/port | Null0 | nexthopip [{slot/port| vlan-id]} [preference]}
Mode: Global Config

Example:

Subnetwork 9.0.0.0/24 is a connected subnetwork in global table and subnet 56.6.6.0/24 is reachable via a gateway 9.0.0.2 in the global table.

Subnet 8.0.0.0/24 is a connected subnetwork in virtual router Red.

Now we leak the 2 routes from global route table into the virtual router Red and leak the connected subnet 8.0.0.0/24 from Red to global table.

When leaking connected route in the global routing table to a virtual router, the /32 host route for the leaked host is added in the virtual router instance’s route table.
Also we add a non-leaked static route for 66.6.6.0/24 subnetwork scoped to the domain of virtual router Red below.

```
(Router) (Config)#ip routing
(Router) (Config)#ip vrf Red
(Router) (Config)#interface 0/27
(Router) (Interface 0/27)#ip address 8.0.0.1 /24
(Router) (Interface 0/27)#routing
(Router) (Interface 0/27)#ip vrf forwarding Red
(Router) (Interface 0/27)#exit

(Router) (Config)#ip route 56.6.6.0 /24 9.0.0.2

Routes leaked from global routing table to VRF’s route table are :
(Router) (Config)#ip route vrf Red 9.0.0.2 255.255.255.255 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 56.6.6.0 255.255.255.0 9.0.0.2 0/26

Route leaked from VRF’s route table to global routing table is :
(Router) (Config)#ip route 8.0.0.2 255.255.255.0 255.255.255.0 0/27

Route (non-leaked) internal to VRF’s route table is :
(Router) (Config)#ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2

5.2.11.1  no ip route
This command deletes a single next hop to a destination static route. If you use the *nexthop* parameter, the next hop is deleted. If you use the *preference* value, the preference value of the static route is reset to its default.

Format  
\[\text{no ip route ipaddr subnetmask [\{nexthop [preference] \| Null0\}\]}\]

Mode  
Global Config

5.2.12  ip route default
This command configures the default route. The value for *nexthop* is a valid IP address of the next hop router. The *preference* is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default  
preference—1

Format  
\[\text{ip route default nexthop [preference]}\]

Mode  
Global Config

5.2.12.1  no ip route default
This command deletes all configured default routes. If the optional *nexthop* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Format  
\[\text{no ip route default [\{nexthop \| preference\}\]}\]

Mode  
Global Config
5.2.13 ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The **ip route** and **ip route default** commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **ip route distance** command.

**Default**

1

**Format**

ip route distance 1-255

**Mode**

Global Config

5.2.13.1 no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

**Format**

no ip route distance

**Mode**

Global Config

5.2.14 ip route net-prototype

This command adds net prototype IPv4 routes to the hardware.

**Format**

ip route net-prototype prefix/prefix-length nexthopip num-routes

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix/prefix-length</td>
<td>The destination network and mask for the route.</td>
</tr>
<tr>
<td>nexthopip</td>
<td>The next-hop ip address, It must belong to an active routing interface, but it does not need to be resolved.</td>
</tr>
<tr>
<td>num-routes</td>
<td>The number of routes need to added into hardware starting from the given prefix argument and within the given prefix-length.</td>
</tr>
</tbody>
</table>
5.2.14.1  no ip route net-prototype
This command deletes all the net prototype IPv4 routes added to the hardware.

**Format**  
`ip route net-prototype prefix/prefix-length nexthopip num-routes`

**Mode**  
Global Config

5.2.15  ip netdirbcast
This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

**Default**  
disabled

**Format**  
`ip netdirbcast`

**Mode**  
Interface Config

5.2.15.1  no ip netdirbcast
This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

**Format**  
`no ip netdirbcast`

**Mode**  
Interface Config

5.2.16  ip mtu
This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the `ip ospf mtu-ignore` command.)

The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see "mtu" on page 291) must take into account the size of the Ethernet header.

For more information about the FASTPATH IP MTU, see the Maximum Transmission Unit in FASTPATH Application Note (document number FASTPATH-AN40X-R).

**Default**  
1500 bytes

**Format**  
`ip mtu 68-12270`

**Mode**  
Interface Config
5.2.16.1 no ip mtu
This command resets the ip mtu to the default value.

Format no ip mtu
Mode Interface Config

5.2.17 encapsulation
This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be ethernet or snap.

Default ethernet
Format encapsulation {ethernet | snap}
Mode Interface Config

 NOTICE
Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

5.2.18 show dhcp lease
This command displays a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. This command does not apply to service or network ports.

Format show dhcp lease [interface slot/port]
Modes Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address, Subnet mask</td>
<td>The IP address and network mask leased from the DHCP server</td>
</tr>
<tr>
<td>DHCP Lease server</td>
<td>The IPv4 address of the DHCP server that leased the address.</td>
</tr>
<tr>
<td>State</td>
<td>State of the DHCPv4 Client on this interface</td>
</tr>
<tr>
<td>DHCP transaction ID</td>
<td>The transaction ID of the DHCPv4 Client</td>
</tr>
<tr>
<td>Lease</td>
<td>The time (in seconds) that the IP address was leased by the server</td>
</tr>
<tr>
<td>Renewal</td>
<td>The time (in seconds) when the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address</td>
</tr>
<tr>
<td>Rebind</td>
<td>The time (in seconds) when the DHCP Rebind process starts</td>
</tr>
<tr>
<td>Retry count</td>
<td>Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds</td>
</tr>
</tbody>
</table>

5.2.19 show ip brief
This command displays the summary information of the IP global configurations, including the ICMP rate limit configuration and the global ICMP Redirect configuration.

Format show ip brief
Modes • Privileged EXEC
• User EXEC
Example: The following shows example CLI display output for the command.

(Switch) #show ip brief

Default Time to Live............................. 64
Routing Mode.................................... Disabled
Maximum Next Hops............................... 4
Maximum Routes.................................. 128
ICMP Rate Limit Interval......................... 1000 msec
ICMP Rate Limit Burst Size....................... 100 messages
ICMP Echo Replies.................................. Enabled
ICMP Redirects..................................... Enabled
System uRPF Mode.................................. Disabled

5.2.20 show ip interface

This command displays all pertinent information about the IP interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Format
show ip interface {slot/port|vlan 1-4093|loopback 0-7}

Modes
• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Interface Status</td>
<td>Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>The primary IP address and subnet masks for the interface. This value appears only if you configure it.</td>
</tr>
<tr>
<td>Method</td>
<td>Shows whether the IP address was configured manually or acquired from a DHCP server.</td>
</tr>
<tr>
<td>Secondary IP Address</td>
<td>One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.</td>
</tr>
<tr>
<td>Helper IP Address</td>
<td>The helper IP addresses configured by the command &quot;ip helper-address (Interface Config)&quot; on page 579.</td>
</tr>
<tr>
<td>Routing Mode</td>
<td>The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.</td>
</tr>
<tr>
<td>Administrative Mode</td>
<td>The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.</td>
</tr>
<tr>
<td>Forward Net Directed Broadcasts</td>
<td>Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.</td>
</tr>
<tr>
<td>Proxy ARP</td>
<td>Displays whether Proxy ARP is enabled or disabled on the system.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(switch)#show ip interface 0/2

Routing Interface Status....................... Down
Primary IP Address............................ 1.2.3.4/255.255.255.0
Method........................................ Manual
Secondary IP Address(es)....................... 21.2.3.4/255.255.255.0
...............................................
Helper IP Address............................ 1.2.3.4
...............................................
1.2.3.5
Routing Mode.................................. Disable
Administrative Mode.......................... Enable
Forward Net Directed Broadcasts............. Disable
Proxy ARP..................................... Enable
Local Proxy ARP.............................. Disable
Active State.................................... Inactive
Link Speed Data Rate.......................... Inactive
MAC Address.................................. 00:10:18:82:0C:68
Encapsulation Type........................... Ethernet
IP MTU........................................ 1500
Bandwidth..................................... 100000 kbps
Destination Unreachables..................... Enabled
ICMP Redirects................................. Enabled
Unicast Reverse Path Forwarding Mode....... Disabled
Unicast Reverse Path Forwarding Allow-Default.. False

Example: In the following example the DHCP client is enabled on a VLAN routing interface.

(Routing) #show ip interface vlan 10

Routing Interface Status....................... Up
Method........................................ DHCP

Term | Definition
--- | ---
Local Proxy ARP | Displays whether Local Proxy ARP is enabled or disabled on the interface.
Active State | Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate | An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address | The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type | The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU | The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth | Shows the bandwidth of the interface.
Destination Unreachables | Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects | Displays whether ICMP Redirects may be sent (enabled or disabled).
DHCP Client Identifier | The client identifier is displayed in the output of the command only if DHCP is enabled with the client-id option on the in-band interface. See “ip address dhcp” on page 516.
Unicast Reverse Path Forwarding Mode | The uRPF mode on the interface.
Unicast Reverse Path Forwarding Allow-Default | Identifies whether the uRPF allow-default parameter has been set.
Routing Mode............................ Enable
Administrative Mode...................... Enable
Forward Net Directed Broadcasts........ Disable
Active State............................ Inactive
Link Speed Data Rate.................... 10 Half
MAC address............................. 00:10:18:82:16:0E
Encapsulation Type...................... Ethernet
IP MTU.................................. 1500
Bandwidth................................ 10000 kbps
Destination Unreachables.............. Enabled
ICMP Redirects......................... Enabled
Interface Suppress Status.............. Unsuppressed
DHCP Client Identifier................ 0fastpath-0010.1882.160E-vl10

5.2.21 show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router, and indicates how each IP address was assigned.

**Format**
show ip interface brief

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>State</td>
<td>Routing operational state of the interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the routing interface in 32-bit dotted decimal format.</td>
</tr>
<tr>
<td>IP Mask</td>
<td>The IP mask of the routing interface in 32-bit dotted decimal format.</td>
</tr>
<tr>
<td>Method</td>
<td>Indicates how each IP address was assigned. The field contains one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• DHCP - The address is leased from a DHCP server.</td>
</tr>
<tr>
<td></td>
<td>• Manual - The address is manually configured.</td>
</tr>
</tbody>
</table>

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

```
(alpha1) #show ip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>IP Address</th>
<th>IP Mask</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/17</td>
<td>Up</td>
<td>192.168.75.1</td>
<td>255.255.255.0</td>
<td>DHCP</td>
</tr>
</tbody>
</table>
```

5.2.22 show ip load-sharing

This command displays the currently configured IP ECMP load balancing mode.

**Format**
show ip load-sharing

**Mode**
Privileged Exec

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

```
(Routing) #show ip load-sharing

ip load-sharing 6 inner
```
5.2.23 show ip protocols

This command lists a summary of the configuration and status for each unicast routing protocol running in the specified virtual router. The command lists routing protocols which are configured and enabled. If a protocol is selected on the command line, the display will be limited to that protocol.

Format

```
show ip protocols [ospf|rip]
```

Mode

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Protocol</td>
<td>OSPFv2.</td>
</tr>
<tr>
<td>Router ID</td>
<td>The router ID configured for OSPFv2.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Whether OSPF is enabled or disabled globally.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>The maximum number of next hops in an OSPF route.</td>
</tr>
<tr>
<td>Routing for Networks</td>
<td>The address ranges configured with an OSPF network command.</td>
</tr>
<tr>
<td>Distance</td>
<td>The administrative distance (or “route preference”) for intra-area, inter-area, and external routes.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>Whether OSPF is configured to originate a default route.</td>
</tr>
<tr>
<td>Always</td>
<td>Whether default advertisement depends on having a default route in the common routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric configured to be advertised with the default route.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>The metric type for the default route.</td>
</tr>
<tr>
<td>Redist Source</td>
<td>A type of routes that OSPF is redistributing.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric to advertise for redistributed routes of this type.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>The metric type to advertise for redistributed routes of this type.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Whether OSPF redistributes subnets of classful addresses, or only classful prefixes.</td>
</tr>
<tr>
<td>Dist List</td>
<td>A distribute list used to filter routes of this type. Only routes that pass the distribute list are redistributed.</td>
</tr>
<tr>
<td>Number of Active Areas</td>
<td>The number of OSPF areas with at least one interface running on this router. Also broken down by area type.</td>
</tr>
<tr>
<td>ABR Status</td>
<td>Whether the router is currently an area border router. A router is an area border router if it has interfaces that are up in more than one area.</td>
</tr>
<tr>
<td>ASBR Status</td>
<td>Whether the router is an autonomous system boundary router. The router is an ASBR if it is redistributing any routes or originating a default route.</td>
</tr>
<tr>
<td>RIP Section</td>
<td>A table showing information for each source protocol (connected, static and ospf). For each of these source the distribution list and metric are shown. Fields which are not configured are left blank. For ospf, configured ospf match parameters are also shown.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interfaces where RIP is enabled and the version sent and accepted on each interface.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(Router) #show ip protocols

Routing Protocol.......................... BGP
Router ID.................................. 6.6.6.6
Local AS Number......................... 65001
BGP Admin Mode.......................... Enable
Maximum Paths............................ Internal 32, External 32
Always compare MED ....................... FALSE
Maximum AS Path Length ................. 75
Fast Internal Failover .................. Enable
Fast External Failover .................. Enable

<table>
<thead>
<tr>
<th>Address</th>
<th>Wildcard</th>
<th>Distance</th>
<th>Pfx List</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.20.0.0</td>
<td>0.0.255.255</td>
<td>40</td>
<td>None</td>
</tr>
<tr>
<td>172.21.0.0</td>
<td>0.0.255.255</td>
<td>45</td>
<td>1</td>
</tr>
</tbody>
</table>

Prefix List In........................ PfxList1
Prefix List Out....................... None

Redistributing:

<table>
<thead>
<tr>
<th>Source</th>
<th>Metric</th>
<th>Dist List</th>
<th>Route Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>connected_list</td>
<td></td>
<td></td>
</tr>
<tr>
<td>static</td>
<td>32120</td>
<td></td>
<td>static_routemap</td>
</tr>
<tr>
<td>rip</td>
<td>30000</td>
<td></td>
<td>rip_routemap</td>
</tr>
<tr>
<td>ospf</td>
<td></td>
<td></td>
<td>ospf_map</td>
</tr>
</tbody>
</table>

Routing for Networks..................

Networks Originated:

10.1.1.0 255.255.255.0 (active)
20.1.1.0 255.255.255.0

Neighbors:

172.20.1.100
Filter List In......................... 1
Filter List Out....................... 2
Prefix List In........................ PfxList2
Prefix List Out....................... PfxList3
Route Map In.......................... rmapUp
Route Map Out........................ rmapDown

Routing Protocol.......................... OSPFv2
Router ID.................................. 6.6.6.6
OSPF Admin Mode.......................... Enable
Maximum Paths............................ 32
Routing for Networks..................

Distance................................. Intra 110 Inter 110 Ext 110

Default Route Advertise................ Disabled
Always.................................... FALSE
Metric..................................... Not configured
Metric Type............................. External Type 2

Redist
Number of Active Areas......................... 3 (3 normal, 0 stub, 0 nssa)
ABR Status...................................... Yes
ASBR Status.................................... Yes

Routing Protocol............................... RIP
RIP Admin Mode............................... Enable
Split Horizon Mode............................ Simple
Default Metric................................. Not configured
Default Route Advertise...................... Disable
Distance......................................... 120

Redistribution:

<table>
<thead>
<tr>
<th>Source</th>
<th>Metric</th>
<th>Dist</th>
<th>List</th>
<th>Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>static</td>
<td>10</td>
<td>15</td>
<td>int ext1 ext2 nssa-ext1</td>
<td></td>
</tr>
<tr>
<td>ospf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Interface

<table>
<thead>
<tr>
<th>Send</th>
<th>Recv</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPv2</td>
<td>RIPv2</td>
</tr>
</tbody>
</table>

5.2.24 show ip route

This command displays the routing table. The ip-address specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The mask specifies the subnet mask for the given ip-address. When you use the longer-prefixes keyword, the ip-address and mask pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the protocol parameter to specify the protocol that installed the routes. The value for protocol can be connected, ospf, rip, static.Use the all parameter to display all routes including best and nonbest routes. If you do not use the all parameter, the command displays only the best route.

| NOTICE | If you use the connected keyword for protocol, the all option is not available because there are no best or nonbest connected routes. |
| NOTICE | If you use the static keyword for protocol, the description option is also available, for example: show ip route ip-address static description. This command shows the description configured with the specified static route(s). |

Format

show ip route [{ip-address [protocol] | {ip-address mask [longer-prefixes] [protocol] | protocol} [all] | all]}

Modes

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Codes</td>
<td>The key for the routing protocol codes that might appear in the routing table output.</td>
</tr>
</tbody>
</table>

The show ip route command displays the routing tables in the following format:

<table>
<thead>
<tr>
<th>Code</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface, Truncated</td>
<td></td>
</tr>
</tbody>
</table>

The columns for the routing table display the following information:
To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type OSPF Inter-Area. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

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

```
(FASTPATH Routing) #show ip route
```

**Route Codes:** R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
L - Leaked Route

Default gateway is 1.1.1.2

```
C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2, 00h:00m:01s, 0/5
C 11.11.11.0/24 [0/1] directly connected, 0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
C 1.1.1.0/24 [0/1] directly connected, Null0
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
C 11.11.11.0/24 [0/1] directly connected, 0/11
S 10.3.2.0/24 [1/0] via 1.1.1.2, 0/11
```

**Example:** The following shows example CLI display output for the command to indicate a truncated route.

```
(router) #show ip route
```

**Route Codes:** R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
L-Leaked Route

Example: The following shows an example of output that displays leaked routes.

Subnetwork 9.0.0.0/24 is a connected subnetwork in global table and subnet 56.6.6.0/24 is reachable via a gateway 9.0.0.2 in the global table. These two routes leak into the virtual router Red and leak the connected subnet 8.0.0.0/24 from Red to global table.

When leaking connected route in the global routing table to a virtual router, the /32 host route for the leaked host is added in the virtual router instance’s route table. Leaking of non /32 connected routes into the virtual router table from global routing table is not supported.

This enables the nodes in subnet 8.0.0.0/24 to access shared services via the global routing table. Also we add a non-leaked static route for 66.6.6.0/24 subnetwork scoped to the domain of virtual router Red.

```
(Router) (Config)#ip route vrf Red 9.0.0.2 255.255.255.255 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 56.6.6.0 255.255.255.0 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2
```

```
(Router) #show ip route vrf Red

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
L - Leaked Route

C 8.0.0.0/24 [0/1] directly connected, 0/27
S L 9.0.0.0/26/32 [1/1] directly connected, 0/26
S L 56.6.6.0/24 [1/1] via 9.0.0.2, 02d:22h:15m, 0/26
S 66.6.6.0/24 [1/1] via 8.0.0.2, 01d:22h:15m, 0/27
```

5.2.25 show ip route ecmp-groups

This command reports all current ECMP groups in the IPv4 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv4 address and outgoing interface of each next hop in each group.

Format show ip route ecmp-groups

Mode Privileged EXEC

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

```
(router) #show ip route ecmp-groups

ECMP Group 1 with 2 next hops (used by 1 route)
172.20.33.100 on interface 2/33
172.20.33.100 on interface 2/34
```

```
ECMP Group 2 with 3 next hops (used by 1 route)
```
5.2.26  show ip route hw-failure

Use this command to display the routes that failed to be added to the hardware due to hash errors or a table full condition.

**Format**  
show ip route hw-failure

**Mode**  
Privileged EXEC

**Example:** The following example displays the command output.

```
(Routing) (Config)#ip route net-prototype 66.6.6.0/24 9.0.0.2 4
```

```
(Routing) #show ip route connected

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
   B - BGP Derived, IA - OSPF Inter Area
   E1 - OSPF External Type 1, E2 - OSPF External Type 2
   N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
   S U - Unnumbered Peer, L - Leaked Route, K - Kernel
   P - Net Prototype

C  9.0.0.0/24 [0/0] directly connected, 0/1
C  8.0.0.0/24 [0/0] directly connected, 0/2
```

```
(Routing) #show ip route hw-failure

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
   B - BGP Derived, IA - OSPF Inter Area
   E1 - OSPF External Type 1, E2 - OSPF External Type 2
   N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
   S U - Unnumbered Peer, L - Leaked Route, K - Kernel
   P - Net Prototype

P  66.6.6.0/24 [1/1] via 9.0.0.2, 01d:22h:15m, 0/1  hw-failure
P  66.6.7.0/24 [1/1] via 9.0.0.2, 01d:22h:15m, 0/1  hw-failure
P  66.6.8.0/24 [1/1] via 9.0.0.2, 01d:22h:15m, 0/1  hw-failure
P  66.6.9.0/24 [1/1] via 9.0.0.2, 01d:22h:15m, 0/1  hw-failure
```

5.2.27  show ip route net-prototype

This command displays the net-prototype routes. The net-prototype routes are displayed with a P.

**Format**  
show ip route net-prototype

**Modes**  
Privileged EXEC

**Example:**

```
(Routing) #show ip route net-prototype

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
   B - BGP Derived, IA - OSPF Inter Area
   E1 - OSPF External Type 1, E2 - OSPF External Type 2
```

show ip route summary

This command displays a summary of the state of the routing table. When the optional all keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

Format

show ip route summary [all]

Modes

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Routes</td>
<td>The total number of connected routes in the routing table.</td>
</tr>
<tr>
<td>Static Routes</td>
<td>Total number of static routes in the routing table.</td>
</tr>
<tr>
<td>RIP Routes</td>
<td>Total number of routes installed by RIP protocol.</td>
</tr>
<tr>
<td>OSPF Routes</td>
<td>Total number of routes installed by OSPF protocol.</td>
</tr>
<tr>
<td>Intra Area Routes</td>
<td>Total number of Intra Area routes installed by OSPF protocol.</td>
</tr>
<tr>
<td>Inter Area Routes</td>
<td>Total number of Inter Area routes installed by OSPF protocol.</td>
</tr>
<tr>
<td>External Type-1 Routes</td>
<td>Total number of External Type-1 routes installed by OSPF protocol.</td>
</tr>
<tr>
<td>External Type-2 Routes</td>
<td>Total number of External Type-2 routes installed by OSPF protocol.</td>
</tr>
<tr>
<td>Reject Routes</td>
<td>Total number of reject routes installed by all protocols.</td>
</tr>
<tr>
<td>Total Routes</td>
<td>Total number of routes in the routing table.</td>
</tr>
<tr>
<td>Best Routes (High)</td>
<td>The number of best routes currently in the routing table. This number only</td>
</tr>
<tr>
<td></td>
<td>counts the best route to each destination. The value in parentheses</td>
</tr>
<tr>
<td></td>
<td>indicates the highest count of unique best routes since counters</td>
</tr>
<tr>
<td></td>
<td>were last cleared.</td>
</tr>
<tr>
<td>Alternate Routes</td>
<td>The number of alternate routes currently in the routing table. An alternate</td>
</tr>
<tr>
<td></td>
<td>route is a route that was not selected as the best route to its</td>
</tr>
<tr>
<td></td>
<td>destination.</td>
</tr>
<tr>
<td>Route Adds</td>
<td>The number of routes that have been added to the routing table.</td>
</tr>
<tr>
<td>Route Modifies</td>
<td>The number of routes that have been changed after they were initially</td>
</tr>
<tr>
<td></td>
<td>added to the routing table.</td>
</tr>
<tr>
<td>Route Deletes</td>
<td>The number of routes that have been deleted from the routing table.</td>
</tr>
<tr>
<td>Unresolved Route Adds</td>
<td>The number of route adds that failed because none of the route's next</td>
</tr>
<tr>
<td></td>
<td>hops were on a local subnet. Note that static routes can fail to be added</td>
</tr>
<tr>
<td></td>
<td>to the routing table at startup because the routing interfaces are not</td>
</tr>
<tr>
<td></td>
<td>yet up. This counter gets incremented in this case. The static routes are</td>
</tr>
<tr>
<td></td>
<td>added to the routing table when the routing interfaces come up.</td>
</tr>
<tr>
<td>Invalid Route Adds</td>
<td>The number of routes that failed to be added to the routing table because</td>
</tr>
<tr>
<td></td>
<td>the route was invalid. A log message is written for each of these failures.</td>
</tr>
<tr>
<td>Failed Route Adds</td>
<td>The number of routes that failed to be added to the routing table because</td>
</tr>
<tr>
<td></td>
<td>of a resource limitation in the routing table.</td>
</tr>
<tr>
<td>Reserved Locals</td>
<td>The number of routing table entries reserved for a local subnet on a</td>
</tr>
<tr>
<td></td>
<td>routing interface that is down. Space for local routes is always reserved</td>
</tr>
<tr>
<td></td>
<td>so that local routes can be installed when a routing interface bounces.</td>
</tr>
<tr>
<td>Unique Next Hops (High)</td>
<td>The number of distinct next hops used among all routes currently in the</td>
</tr>
<tr>
<td></td>
<td>routing table. These include local interfaces for local routes and</td>
</tr>
<tr>
<td></td>
<td>neighbors for indirect routes. The value in parentheses indicates the</td>
</tr>
<tr>
<td></td>
<td>highest count of unique next hops since counters were last cleared.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

```
(Routing) #show ip route summary
Connected Routes............................ 7
Static Routes.................................. 1
RIP Routes..................................... 20
BGP Routes..................................... 10
    External.................................. 0
    Internal.................................. 10
    Local...................................... 0
OSPF Routes................................... 1004
    Intra Area Routes......................... 4
    Inter Area Routes......................... 1000
    External Type-1 Routes.................... 0
    External Type-2 Routes.................... 0
Reject Routes.................................. 0
Total routes.................................. 1032

Best Routes (High)............................ 1032 (1032)
Alternate Routes.............................. 0
Route Adds.................................... 1010
Route Modifies................................. 1
Route Deletes.................................. 10
Unresolved Route Adds......................... 0
Invalid Route Adds............................. 0
Failed Route Adds............................. 0
Reserved Locals................................. 0

Unique Next Hops (High)........................ 13 (13)
Next Hop Groups (High)......................... 13 (14)
ECMP Groups (High)............................. 2 (3)
ECMP Routes.................................. 1001
Truncated ECMP Routes........................ 0
ECMP Retries.................................. 0
Routes with 1 Next Hop........................ 31
Routes with 2 Next Hops......................... 1
Routes with 4 Next Hops........................ 1000
```
5.2.29  clear ip route counters
The command resets to zero the IPv4 routing table counters reported in the command “show ip route summary” on page 532. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format  clear ip route counters
Mode     Privileged EXEC

5.2.30  show ip route preferences
This command displays detailed information about the route preferences for each type of route. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format  show ip route preferences
Modes   •  Privileged EXEC
         •  User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>The local route preference value.</td>
</tr>
<tr>
<td>Static</td>
<td>The static route preference value.</td>
</tr>
<tr>
<td>OSPF Intra</td>
<td>The OSPF Intra route preference value.</td>
</tr>
<tr>
<td>OSPF Inter</td>
<td>The OSPF Inter route preference value.</td>
</tr>
<tr>
<td>OSPF External</td>
<td>The OSPF External route preference value.</td>
</tr>
<tr>
<td>RIP</td>
<td>The RIP route preference value.</td>
</tr>
<tr>
<td>Configured Default Gateway</td>
<td>The route preference value of the statically-configured default gateway.</td>
</tr>
<tr>
<td>DHCP Default Gateway</td>
<td>The route preference value of the default gateway learned from the DHCP server.</td>
</tr>
</tbody>
</table>

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

(alpha-stack) #show ip route preferences

Local.......................................... 0
Static......................................... 1
OSPF Intra.................................... 110
OSPF Inter.................................... 110
OSPF External.................................. 110
RIP............................................ 120
Configured Default Gateway............ 253
DHCP Default Gateway..................... 254

5.2.31  show ip stats
This command displays IP statistical information.

Format  show ip stats
Modes   •  Privileged EXEC
         •  User EXEC
5.2.32 show routing heap summary

This command displays a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing applications.

**Format**
show routing heap summary

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heap Size</td>
<td>The amount of memory, in bytes, allocated at startup for the routing heap.</td>
</tr>
<tr>
<td>Memory In Use</td>
<td>The number of bytes currently allocated.</td>
</tr>
<tr>
<td>Memory on Free List</td>
<td>The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.</td>
</tr>
<tr>
<td>Memory Available in Heap</td>
<td>The number of bytes in the original heap that have never been allocated.</td>
</tr>
<tr>
<td>In Use High Water Mark</td>
<td>The maximum memory in use since the system last rebooted.</td>
</tr>
</tbody>
</table>

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

```
(ROUTER) #show routing heap summary
Heap Size....................... 95053184
Memory In Use................... 56998
Memory on Free List.............. 47
Memory Available in Heap...... 94996170
In Use High Water Mark........ 57045
```

5.3 Routing Policy Commands

5.3.1 ip policy route-map

Use this command to identify a route map to use for policy-based routing on an interface specified by route-map-name. Policy-based routing is configured on the interface that receives the packets, not on the interface from which the packets are sent.

When a route-map applied on the interface is changed, that is, if new statements are added to route-map or match/set terms are added/removed from route-map statement, and also if route-map that is applied on an interface is removed, route-map needs to be removed from interface and added back again in order to have changed route-map configuration to be effective.

---

**NOTICE**
Route-map and Diffserv cannot work on the same interface.

**Example:** The following is an example of this command.

```
(FASTPATH Routing) (Config)#interface 0/1
(FASTPATH Routing) (Interface 0/1)#
(FASTPATH Switching) (Interface 0/1)# #ip policy route-map equal-access
```

In order to disable policy based routing from an interface, use no form of this command
```
no ip policy <route-map-name>
```
5.3.2 ip prefix-list

To create a prefix list or add a prefix list entry, use the ip prefix-list command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route’s prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assume if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route’s prefix using the command “match ip address” on page 539.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

Default

No prefix lists are configured by default. When neither the ge nor the le option is configured, the destination prefix must match the network/length exactly. If the ge option is configured without the le option, any prefix with a network mask greater than or equal to the ge value is considered a match. Similarly, if the le option is configured without the ge option, a prefix with a network mask less than or equal to the le value is considered a match.

Format

```
ip prefix-list list-name {[seq number] {permit | deny} network/length [ge length] [le length] | renumber renumber-interval first-statement-number}
```

Mode

Global Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>The text name of the prefix list. Up to 32 characters.</td>
</tr>
<tr>
<td>seq number</td>
<td>(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.</td>
</tr>
<tr>
<td>permit</td>
<td>Permit routes whose destination prefix matches the statement.</td>
</tr>
<tr>
<td>deny</td>
<td>Deny routes whose destination prefix matches the statement.</td>
</tr>
<tr>
<td>network/length</td>
<td>Specifies the match criteria for routes being compared to the prefix list statement. The network can be any valid IP prefix. The length is any IPv4 prefix length from 0 to 32.</td>
</tr>
<tr>
<td>ge length</td>
<td>(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.</td>
</tr>
<tr>
<td>le length</td>
<td>(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the ge length and less than or equal to 32.</td>
</tr>
<tr>
<td>renumber</td>
<td>(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for renumber-interval is 1–100, and the valid range for first-statement-number is 1–1000.</td>
</tr>
</tbody>
</table>

Example: The following example configures a prefix list that allows routes with one of two specific destination prefixes, 172.20.0.0/16 and 192.168.1.0/24:

(Routing)(config)# ip prefix-list apple seq 10 permit 172.20.0.0/16
(Routing)(config)# ip prefix-list apple seq 20 permit 192.168.10.24

Example: The following example disallows only the default route.

(Routing)(config)# ip prefix-list orange deny 0.0.0.0/0
(Routing)(config)# ip prefix-list orange permit 0.0.0.0/0 ge 1
5.3.2.1 **no ip prefix-list**
To delete a prefix list or a statement in a prefix list, use the no form of this command. The command no ip prefix-list list-name deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

**Format**
```
no ip prefix-list list-name [seq number] { permit | deny } network/length [ge length] [le length]
```

**Mode**
Global Configuration

5.3.3 **ip prefix-list description**
To apply a text description to a prefix list, use the ip prefix-list description command in Global Configuration mode.

**Default**
No description is configured by default.

**Format**
```
ip prefix-list list-name description text
```

**Mode**
Global Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>The text name of the prefix list.</td>
</tr>
<tr>
<td>description text</td>
<td>Text description of the prefix list. Up to 80 characters.</td>
</tr>
</tbody>
</table>

5.3.3.1 **no ip prefix-list description**
To remove the text description, use the no form of this command.

**Format**
```
no ip prefix-list list-name description
```

**Mode**
Global Configuration

5.3.4 **ipv6 prefix-list**
Use this command to create IPv6 prefix lists. An IPv6 prefix list can contain only ipv6 addresses. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. For IPv6 routes, only IPv6 prefix lists are matched. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. An IPv6 prefix list may be used within a route map to match a route's prefix using the `match ipv6 address` command. A route map may contain both IPv4 and IPv4 prefix lists. If a route being matched is an IPv6 route, only the IPv6 prefix lists are matched.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64. These numbers indicate only IPv6 prefix lists. IPv4 prefix lists may be configured in appropriate numbers independently.

**Default**
No prefix lists are configured by default. When neither the ge nor the le option is configured, the destination prefix must match the network/length exactly. If the ge option is configured without the le option, any prefix with a network mask greater than or equal to the ge value is considered a match. Similarly, if the le option is configured without the ge option, a prefix with a network mask less than or equal to the le value is considered a match.

**Format**
```
ipv6 prefix-list list-name [seq seq-number] { (permit/deny) ipv6-prefix/prefix-length [ge ge-value] [le le-value] | description text | renumber renumber-interval first-statement-number}
```

**Mode**
Global Configuration
### Example:
The following example configures a prefix list that allows routes with one of two specific destination prefixes, 2001::/64 and 5F00::/48:

```
(R1)(config)# ipv6 prefix-list apple seq 10 permit 2001::/64
(R1)(config)# ipv6 prefix-list apple seq 20 permit 5F00::/48
```

### 5.3.4.1 no ipv6 prefix-list

Use this command to deletes either the entire prefix list or an individual statement from a prefix list.

**Format**

```
ipv6 prefix-list list-name
```

**Mode**

Global Configuration

---

**NOTICE**

The description must be removed using `no ip prefix-list description` before using this command to delete an IPv6 Prefix List.

### 5.3.5 route-map

To create a route map and enter Route Map Configuration mode, use the `route-map` command in Global Configuration mode. One use of a route map is to limit the redistribution of routes to a specified range of route prefixes. The redistribution command specifies a route map which refers to a prefix list. The prefix list identifies the prefixes that may be redistributed. FASTPATH accepts up to 64 route maps.

**Default**

No route maps are configured by default. If no permit or deny tag is given, `permit` is the default.

**Format**

```
route-map map-tag [permit|deny] [sequence-number]
```

**Mode**

Global Configuration
Example: In the following example, BGP is configured to redistribute the all prefixes within 172.20.0.0 and reject all others.

```plaintext
(Routing)(config)# ip prefix-list redist-pl permit 172.20.0.0/16 le 32
(Routing)(config)# route-map redist-rm permit
(Routing)(config-route-map)# match ip address prefix-list redist-pl
(Routing)(config-route-map)# exit
(Routing)(config) router bgp 1
(Routing)(Config-router) redistribute ospf route-map redist-rm
```

5.3.5.1 no route-map

To delete a route map or one of its statements, use the no form of this command.

```
Format no route-map map-tag [permit|deny] [sequence-number]
Mode Global Configuration
```

5.3.6 match ip address

To configure a route map to match based on a destination prefix, use the match ip address command in Route Map Configuration mode. If you specify multiple prefix lists in one statement, then a match occurs if a prefix matches any one of the prefix lists. If you configure a match ip address statement within a route map section that already has a match ip address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

Default No match criteria are defined by default.

```
Format match ip address prefix-list prefix-list-name [prefix-list-name...]
Mode Route Map Configuration
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-list-name</td>
<td>The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.</td>
</tr>
</tbody>
</table>
5.3.6.1 no match ip address
To delete a match statement from a route map, use the no form of this command.

Format       no match ip address [prefix-list prefix-list-name [prefix-list-name...]]
Mode         Route Map Configuration

5.3.7 match ip address <access-list-number | access-list-name>
Use this command to configure a route map in order to match based on the match criteria configured in an IP access-list.
Note that an IP ACL must be configured before it is linked to a route-map. Actions present in an IP ACL configuration are applied with other actions involved in route-map. If an IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

If there are a list of IP access-lists specified in this command and the packet matches at least one of these access-list match criteria, the corresponding set of actions in route-map are applied to packet.

If there are duplicate IP access-list numbers/names in this command, the duplicate configuration is ignored.

Default       No match criteria are defined by default.
Format         match ip address access-list-number | access-list-name [...access-list-number | name ]
Mode           Route Map Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-list-number</td>
<td>The access-list number that identifies an access-list configured through access-list CLI configuration commands. This number is 1 to 99 for standard access list number. This number is 100 to 199 for extended access list number.</td>
</tr>
<tr>
<td>Access-list-name</td>
<td>The access-list name that identifies named IP ACLs. Access-list name can be up to 31 characters in length. A maximum of 16 ACLs can be specified in this 'match' clause.</td>
</tr>
</tbody>
</table>

**Example:** The following sequence shows creating a route-map with “match” clause on ACL number and applying that route-map on an interface.

```
(config)#access-list 1 permit ip 10.1.0.0 0.0.255.255
(config)#access-list 2 permit ip 10.2.0.0 0.0.255.255
(config)#route-map equal-access permit 10
(config)#route-map#match ip address 1
(config)#route-map#set ip default next-hop 192.168.6.6
(config)#route-map#route-map equal-access permit 20
(config)#route-map#match ip address 2
(config)#route-map#set ip default next-hop 172.16.7.7
(config)#interface 0/1
(config)#interface 0/1#ip address 10.1.1.1 255.255.255.0
(config)#interface 0/1#ip policy route-map equal-access
(config)#interface 0/2
(config)#interface 0/2#ip address 192.168.6.5 255.255.255.0
(config)#interface 0/3
(config)#interface 0/3#ip address 172.16.7.6 255.255.255.0
```

The ip policy route-map equal-access command is applied to interface 0/1. All packets coming inside 0/1 are policy-routed.

Sequence number 10 in route map equal-access is used to match all packets sourced from any host in subnet 10.1.0.0. If there is a match, and if the router has no explicit route for the packet’s destination, it is sent to next-hop address 192.168.6.6.

Sequence number 20 in route map equal-access is used to match all packets sourced from any host in subnet 10.2.0.0. If there is a match, and if the router has no explicit route for the packet’s destination, it is sent to next-hop address 172.16.7.7.

Rest all packets are forwarded as per normal L3 destination-based routing.
**Example:** This example illustrates the scenario where IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, this is how configuration is rejected:

(FASTPATH Routing) #show ip access-lists

Current number of ACLs: 9  Maximum number of ACLs: 100

<table>
<thead>
<tr>
<th>ACL ID/Name</th>
<th>Rules</th>
<th>Direction</th>
<th>Interface(s)</th>
<th>VLAN(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>madan</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(FASTPATH Routing) #show mac access-lists

Current number of all ACLs: 9  Maximum number of all ACLs: 100

<table>
<thead>
<tr>
<th>MAC ACL Name</th>
<th>Rules</th>
<th>Direction</th>
<th>Interface(s)</th>
<th>VLAN(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>madan</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mohan</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>goud</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(FASTPATH Routing) #
(FASTPATH Routing) #
(FASTPATH Routing) #configure

(FASTPATH Routing) (Config)#route-map madan

(FASTPATH Routing) (route-map)#match ip address 1 2 3 4 5 madan

(FASTPATH Routing) (route-map)#match mac-list madan mohan goud

(FASTPATH Routing) (route-map)#exit

(FASTPATH Routing) (Config)#exit

(FASTPATH Routing) #show route-map

route-map madan permit 10

Match clauses:
    ip address (access-lists) : 1 2 3 4 5 madan
    mac-list (access-lists) : madan mohan goud

Set clauses:

(FASTPATH Routing) (Config)#access-list 2 permit every

Request denied. Another application using this ACL restricts the number of rules allowed.

(FASTPATH Routing) (Config)#ip access-list madan

(FASTPATH Routing) (Config-ipv4-acl)#permit udp any any

Request denied. Another application using this ACL restricts the number of rules allowed.
5.3.7.1  no match ip address
To delete a match statement from a route map, use the no form of this command.

Format  no match ip address [access-list-number | access-list-name]
Mode     Route Map Configuration

5.3.8  match ipv6 address
Use this command to configure a route map to match based on a destination prefix. prefix-list prefix-list-name identifies the name of an IPv6 prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified. If multiple prefix lists are specified, a match occurs if a prefix matches any one of the prefix lists. If you configure a match ipv6 address statement within a route map section that already has a match ipv6 address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

Default  No match criteria are defined by default.
Format   match ipv6 address prefix-list prefix-list-name [prefix-list-name...]
Mode     Route Map Configuration

Example: In the example below, IPv6 addresses specified by the prefix list apple are matched through the route map abc.
Router(config)# route-map abc
Router(config-route-map)# match ipv6 address prefix-list apple

5.3.8.1  no match ipv6 address
To delete a match statement from a route map, use the no form of this command.

Format  no match ipv6 address prefix-list prefix-list-name [prefix-list-name...]
Mode     Route Map Configuration

5.3.9  match length
Use this command to configure a route map to match based on the Layer 3 packet length between specified minimum and maximum values. min specifies the packet’s minimum Layer 3 length, inclusive, allowed for a match. max specifies the packet’s maximum Layer 3 length, inclusive, allowed for a match. Each route-map statement can contain one 'match' statement on packet length range.

Default  No match criteria are defined by default.
Format   match length min max
Mode     Route Map Configuration

Example: The following shows an example of the command.
(Routing) (config-route-map)# match length 64 1500
5.3.9.1 no match length
Use this command to delete a match statement from a route map.

**Format**
no match length

**Mode**
Route Map Configuration

5.3.10 match mac-list
Use this command to configure a route map in order to match based on the match criteria configured in an MAC access-list.

A MAC ACL is configured before it is linked to a route-map. Actions present in MAC ACL configuration are applied with other actions involved in route-map. When a MAC ACL referenced by a route-map is removed, the route-map rule is also removed and the corresponding rule is not effective. When a MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

**Default**
No match criteria are defined by default.

**Format**
match mac-list mac-list-name [mac-list-name]

**Mode**
Route Map Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-list-name</td>
<td>The mac-list name that identifies MAC ACLs. MAC Access-list name can be up to 31 characters in length.</td>
</tr>
</tbody>
</table>

**Example:** The following is an example of the command.

(FASTPATH Routing) (config-route-map)# match mac-list MacList1

Example 2: This example illustrates the scenario where MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL, this is how configuration is rejected:

FASTPATH Routing) #show mac access-lists

Current number of all ACLs: 9  Maximum number of all ACLs: 100

<table>
<thead>
<tr>
<th>MAC ACL Name</th>
<th>Rules</th>
<th>Direction</th>
<th>Interface(s)</th>
<th>VLAN(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>madan</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mohan</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>goud</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(FASTPATH Routing) #
(FASTPATH Routing) #
(FASTPATH Routing) #configure

(FASTPATH Routing) (Config)#route-map madan

(FASTPATH Routing) (route-map)#match mac-list madan mohan goud

(FASTPATH Routing) (route-map)#exit

(FASTPATH Routing) (Config)#exit

(FASTPATH Routing) #show route-map

route-map madan permit 10
   Match clauses:
mac-list (access-lists) : madan mohan goud
Set clauses:

(FASTPATH Routing) (Config)#mac access-list extended madan

(FASTPATH Routing) (Config-mac-access-list)#permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:ff any

Request denied. Another application using this ACL restricts the number of rules allowed.

5.3.10.1 no match mac-list
To delete a match statement from a route map, use the no form of this command.

Format no match mac-list [mac-list-name]
Mode Route Map Configuration

5.3.11 set interface
If network administrator does not want to revert to normal forwarding but instead want to drop a packet that does not match the specified criteria, a set statement needs to be configured to route the packets to interface null0 as the last entry in the route-map. set interface null0 needs to be configured in a separate statement. It should not be added along with any other statement having other match/set terms.

A route-map statement that is used for PBR is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet meeting the match criteria. If the statement is marked as permit, and if the packet meets all the match criteria, then set commands in the route-map statement are applied. If no match is found in the route-map, the packet is not dropped, instead the packet is forwarded using the routing decision taken by performing destination-based routing.

Format set interface null0
Mode Route Map Configuration

5.3.12 set ip next-hop
Use this command to specify the adjacent next-hop router in the path toward the destination to which the packets should be forwarded. If more than one IP address is specified, the first IP address associated with a currently up-connected interface is used to route the packets.

This command affects all incoming packet types and is always used if configured. If configured next-hop is not present in the routing table, an ARP request is sent from the router.

In a route-map statement, ‘set ip next-hop’ and ‘set ip default next-hop’ terms are mutually exclusive. However, a ‘set ip default next-hop’ can be configured in a separate route-map statement.

Format set ip next-hop ip-address [...ip-address]
Mode Route Map Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this ‘set’ clause.</td>
</tr>
</tbody>
</table>
5.3.12.1 no set ip next-hop
Use this command to remove a set command from a route map.

Format: no set ip next-hop ip-address [...ip-address]
Mode: Route Map Configuration

5.3.13 set ip default next-hop
Use this command to set a list of default next-hop IP addresses. If more than one IP address is specified, the first next hop specified that appears to be adjacent to the router is used. The optional specified IP addresses are tried in turn.
A packet is routed to the next hop specified by this command only if there is no explicit route for the packet’s destination address in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.
In a route-map statement, ‘set ip next-hop’ and ‘set ip default next-hop’ terms are mutually exclusive. However, a ‘set ip next-hop’ can be configured in a separate route-map statement

Format: set ip default next-hop ip-address [...ip-address]
Mode: Route Map Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this ‘set’ clause.</td>
</tr>
</tbody>
</table>

5.3.13.1 no set ip default next-hop
Use this command to remove a set command from a route map.

Format: no set ip default next-hop ip-address [...ip-address]
Mode: Route Map Configuration

5.3.14 set ip precedence
Use this command to set the three IP precedence bits in the IP packet header. With three bits, you have eight possible values for the IP precedence; values 0 through 7 are defined. This command is used when implementing QoS and can be used by other QoS services, such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

Format: set ip precedence 0-7
Mode: Route Map Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Sets the routine precedence</td>
</tr>
<tr>
<td>1</td>
<td>Sets the priority precedence</td>
</tr>
<tr>
<td>2</td>
<td>Sets the immediate precedence</td>
</tr>
<tr>
<td>3</td>
<td>Sets the Flash precedence</td>
</tr>
<tr>
<td>4</td>
<td>Sets the Flash override precedence</td>
</tr>
<tr>
<td>5</td>
<td>Sets the critical precedence</td>
</tr>
<tr>
<td>6</td>
<td>Sets the internetwork control precedence</td>
</tr>
<tr>
<td>7</td>
<td>Sets the network control precedence</td>
</tr>
</tbody>
</table>
5.3.14.1 **no set ip precedence**

Use this command to reset the three IP precedence bits in the IP packet header to the default.

**Format**

```
no set ip precedence
```

**Mode**

Route Map Configuration

---

5.3.15 **show ip policy**

This command lists the route map associated with each interface.

**Format**

```
show ip policy
```

**Mode**

Privileged EXEC

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface.</td>
</tr>
<tr>
<td>Route-map</td>
<td>The route map</td>
</tr>
</tbody>
</table>

---

5.3.16 **show ip prefix-list**

This command displays configuration and status for a prefix list.

**Format**

```
show ip prefix-list [detail | summary] [prefix-list-name [network/length] [seq sequence-number] [longer] [first-match]
```

**Mode**

Privileged EXEC

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed or summarized information about all prefix lists.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays detailed or summarized information about all prefix lists.</td>
</tr>
<tr>
<td>prefix-list-name</td>
<td>(Optional) The name of a specific prefix list.</td>
</tr>
<tr>
<td>network/length</td>
<td>(Optional) The network number and length (in bits) of the network mask.</td>
</tr>
<tr>
<td>seq</td>
<td>(Optional) Applies the sequence number to the prefix list entry.</td>
</tr>
<tr>
<td>sequence-number</td>
<td>(Optional) The sequence number of the prefix list entry.</td>
</tr>
<tr>
<td>longer</td>
<td>(Optional) Displays all entries of a prefix list that are more specific than the given network/length.</td>
</tr>
<tr>
<td>first-match</td>
<td>(Optional) Displays the entry of a prefix list that matches the given network/length.</td>
</tr>
</tbody>
</table>

Acceptable forms of this command are as follows:
- `show ip prefix-list prefix-list-name network/length first-match`
- `show ip prefix-list prefix-list-name network/length longer`
- `show ip prefix-list prefix-list-name network/length`
- `show ip prefix-list prefix-list-name seq sequence-number`
- `show ip prefix-list prefix-list-name`
- `show ip prefix-list summary`
- `show ip prefix-list summary prefix-list-name`
- `show ip prefix-list detail`
- `show ip prefix-list detail prefix-list-name`
**Example:** The following shows example CLI display output for the command.

(Routing) #show ip prefix-list fred

```bash
ip prefix-list fred:
  count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
  seq 5 permit 10.10.1.1/20 ge 22
  seq 10 permit 10.10.1.2/20 le 30
  seq 15 permit 10.10.1.2/20 ge 29 le 30
```

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

(Routing) #show ip prefix-list summary fred

```bash
ip prefix-list fred:
  count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
```

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

(Routing) #show ip prefix-list detail fred

```bash
ip prefix-list fred:
  count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
  seq 5 permit 10.10.1.1/20 ge 22 (hitcount: 0)
  seq 10 permit 10.10.1.2/20 le 30 (hitcount: 0)
  seq 15 permit 10.10.1.2/20 ge 29 le 30 (hitcount: 0)
```

### 5.3.17 **show ipv6 prefix-list**

This command displays configuration and status for a selected prefix list.

**Format**

```
show ipv6 prefix-list [detail | summary] listname [ipv6-prefix/prefix-length] [seq sequence-number] [longer] [first-match]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>summary</td>
</tr>
<tr>
<td>list-name</td>
<td>(Optional) The name of a specific prefix list.</td>
</tr>
<tr>
<td>ipv6-prefix/prefix-length</td>
<td>(Optional) The network number and length (in bits) of the network mask.</td>
</tr>
<tr>
<td>seq</td>
<td>(Optional) Applies the sequence number to the prefix list entry.</td>
</tr>
<tr>
<td>sequence-number</td>
<td>(Optional) The sequence number of the prefix list entry.</td>
</tr>
<tr>
<td>longer</td>
<td>(Optional) Displays all entries of a prefix list that are more specific than the given network/length.</td>
</tr>
<tr>
<td>first-match</td>
<td>(Optional) Displays the entry of a prefix list that matches the given network/length.</td>
</tr>
</tbody>
</table>

Acceptable forms of this command are as follows:

- `show ipv6 prefix-list listname ipv6-prefix/prefix-length first-match`
- `show ipv6 prefix-list listname ipv6-prefix/prefix-length longer`
- `show ipv6 prefix-list listname ipv6-prefix/prefix-length`
- `show ipv6 prefix-list listname seq sequence-number`
- `show ipv6 prefix-list listname`
- `show ipv6 prefix-list summary`
- `show ipv6 prefix-list summary prefix-list-name`
- `show ipv6 prefix-list detail`
- `show ipv6 prefix-list detail prefix-list-name`

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

(Switch) #show ipv6 prefix-list apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
seq 5 deny 5F00::/8 le 128
seq 10 deny ::/0
seq 15 deny ::/1
seq 20 deny ::/2
seq 25 deny ::/3 ge 4
   seq 30 permit ::/0 le 128

(Switch) #show ipv6 prefix-list summary apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31

(Switch) #show ipv6 prefix-list detail apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
seq 10 deny ::/0 (hit count: 0, refcount: 1)
seq 15 deny ::/1 (hit count: 0, refcount: 1)
seq 20 deny ::/2 (hit count: 0, refcount: 1)
seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)

5.3.18 show route-map
To display a route map, use the show route-map command in Privileged EXEC mode.

Format
show route-map [map-name]

Mode
Privileged EXEC

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

(Routing) # show route-map test
route-map test, permit, sequence 10
  Match clauses:
   ip address prefix-lists: orange
  Set clauses:
   set metric 50
5.3.19 clear ip prefix-list

To reset IP prefix-list counters, use the clear ip prefix-list command in Privileged EXEC mode. This command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

**Format**

```
clear ip prefix-list [prefix-list-name] [network/length]
```

**Mode**

Privileged EXEC

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-list-name</td>
<td>(Optional) Name of the prefix list from which the hit count is to be cleared.</td>
</tr>
<tr>
<td>network/length</td>
<td>(Optional) Network number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.</td>
</tr>
</tbody>
</table>

**Example:**
The following shows an example of the command.

(Routing) # clear ip prefix-list orange 20.0.0.0/8

5.3.20 clear ipv6 prefix-list

Use this command to reset and clear IPv6 prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

**Format**

```
clear ipv6 prefix-list [prefix-list-name] [ipv6-prefix/prefix-length]
```

**Mode**

Privileged EXEC

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>(Optional) Name of the prefix list from which the hit count is to be cleared.</td>
</tr>
<tr>
<td>ipv6-prefix/prefix-length</td>
<td>(Optional) IPv6 prefix number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.</td>
</tr>
</tbody>
</table>

5.4 Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

5.4.1 ip irdp

This command enables Router Discovery on an interface or range of interfaces.

**Default**

```
disabled
```

**Format**

```
ip irdp
```

**Mode**

Interface Config
5.4.1  no ip irdp
This command disables Router Discovery on an interface.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip irdp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

5.4.2  ip irdp address
This command configures the address that the interface uses to send the router discovery advertisements. The valid values for ipaddr are 224.0.0.1, which is the all-hosts IP multicast address, and 255.255.255.255, which is the limited broadcast address.

<table>
<thead>
<tr>
<th>Default</th>
<th>224.0.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip irdp address ipaddr</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

5.4.2.1  no ip irdp address
This command configures the default address used to advertise the router for the interface.

| Format      | no ip irdp address |
|-------------| Interface Config |

5.4.3  ip irdp holdtime
This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of 4 to 9000 seconds.

<table>
<thead>
<tr>
<th>Default</th>
<th>3 * maxinterval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip irdp holdtime 4-9000</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

5.4.3.1  no ip irdp holdtime
This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

| Format      | no ip irdp holdtime |
|-------------| Interface Config |

5.4.4  ip irdp maxadvertinterval
This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for maxadvertinterval is 4 to 1800 seconds.

<table>
<thead>
<tr>
<th>Default</th>
<th>600</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip irdp maxadvertinterval 4-1800</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>
5.4.4.1   no ip irdp maxadvertinterval
This command configures the default maximum time, in seconds.

Format       no ip irdp maxadvertinterval
Mode         Interface Config

5.4.5   ip irdp minadvertinterval
This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is 3–1800.

Default      0.75 * maxadvertinterval
Format       ip irdp minadvertinterval 3-1800
Mode         Interface Config

5.4.5.1   no ip irdp minadvertinterval
This command sets the default minimum time to the default.

Format       no ip irdp minadvertinterval
Mode         Interface Config

5.4.6   ip irdp multicast
This command configures the destination IP address for router advertisements as 224.0.0.1, which is the default address. The no form of the command configures the IP address as 255.255.255.255 to instead send router advertisements to the limited broadcast address.

Format       ip irdp multicast ip address
Mode         Interface Config

5.4.6.1   no ip irdp multicast
By default, router advertisements are sent to 224.0.0.1. To instead send router advertisements to the limited broadcast address, 255.255.255.255, use the no form of this command.

Format       no ip irdp multicast
Mode         Interface Config

5.4.7   ip irdp preference
This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.

Default      0
Format       ip irdp preference -2147483648 to 2147483647
Mode         Interface Config
5.4.7.1 **no ip irdp preference**

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

**Format**
```
no ip irdp preference
```

**Mode**
```
Interface Config
```

5.4.8 **show ip irdp**

This command displays the router discovery information for all interfaces, a specified interface, or specified VLAN. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of in a `slot/port` format.

**Format**
```
show ip irdp {slot/port|vlan 1-4093|all}
```

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The <code>slot/port</code> that corresponds to a physical routing interface or vlan routing interface.</td>
</tr>
<tr>
<td>vlan</td>
<td>Use this keyword to specify the VLAN ID of the routing VLAN directly instead of in a <code>slot/port</code> format.</td>
</tr>
<tr>
<td>Ad Mode</td>
<td>The advertise mode, which indicates whether router discovery is enabled or disabled on this interface.</td>
</tr>
<tr>
<td>Dest Address</td>
<td>The destination IP address for router advertisements.</td>
</tr>
<tr>
<td>Max Int</td>
<td>The maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.</td>
</tr>
<tr>
<td>Min Int</td>
<td>The minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The amount of time, in seconds, that a system should keep the router advertisement before discarding it.</td>
</tr>
<tr>
<td>Preference</td>
<td>The preference of the address as a default router address, relative to other router addresses on the same subnet.</td>
</tr>
</tbody>
</table>

5.5 **Virtual LAN Routing Commands**

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

5.5.1 **vlan routing**

This command enables routing on a VLAN. The `vlanid` value has a range from 1 to 4093. The `[interface ID]` value has a range from 1 to 128. Typically, you will not supply the interface ID argument, and the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the `slot/port` for the VLAN routing interface. If you select an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface. For products that use text-based configuration, including the interface ID in the vlan routing command for the text configuration ensures that the `slot/port` for the VLAN interface stays the same across a restart. Keeping the `slot/port` the same ensures that the correct interface configuration is applied to each interface when the system restarts.

**Format**
```
vlan routing vlanid [interface ID]
```

**Mode**
```
VLAN Config
```
5.5.1.1 no vlan routing

This command deletes routing on a VLAN.

**Format**

no vlan routing vlanid

**Mode**

VLAN Config

**Example:** Example 1 shows the command specifying a vlanid value. The interface ID argument is not used.

```
(Switch)(Vlan)#vlan 14
(Switch)(Vlan)#vlan routing 14 ?
<cr>
Press enter to execute the command.
<1-24>
```

Typically, you press <Enter> without supplying the Interface ID value; the system automatically selects the interface ID.

**Example:** In Example 2, the command specifies interface ID 51 for VLAN 14 interface. The interface ID becomes the port number in the slot/port for the VLAN routing interface. In this example, slot/port is 4/51 for VLAN 14 interface.

```
(Switch)(Vlan)#vlan 14 51
(Switch)(Vlan)#
```

**Example:** In Example 3, you select an interface ID that is already in use. In this case, the CLI displays an error message and does not create the VLAN interface.

```
(Switch)#config
(Switch)(Config)#exit
(Switch)#vlan database
(Switch)(Vlan)#vlan 15
(Switch)(Vlan)#vlan routing 15 1
```

**Example:** The show running configuration command always lists the interface ID for each routing VLAN, as shown in Example 4 below.

```
(Switch) #show running-config
!!Current Configuration:
```

MAC Address used by Routing VLANs: 00:11:88:59:47:36

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4/1</td>
<td>172.16.10.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>11</td>
<td>4/50</td>
<td>172.16.11.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>12</td>
<td>4/3</td>
<td>172.16.12.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>13</td>
<td>4/4</td>
<td>172.16.13.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>14</td>
<td>4/51</td>
<td>0.0.0.0</td>
<td>0.0.0.0 &lt;---u/s/p is 4/51 for VLAN 14 interface</td>
</tr>
</tbody>
</table>

MAC Address used by Routing VLANs: 00:11:88:59:47:36

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4/1</td>
<td>172.16.10.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>11</td>
<td>4/50</td>
<td>172.16.11.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>12</td>
<td>4/3</td>
<td>172.16.12.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>13</td>
<td>4/4</td>
<td>172.16.13.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>14</td>
<td>4/51</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>
5.5.2 interface vlan

Use this command to enter Interface configuration mode for the specified VLAN. The vlan-id range is 1 to 4093.

Format  interface vlan vlan-id
Mode    Global Config

5.5.3 show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format  show ip vlan
Modes   • Privileged EXEC
        • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address used by</td>
<td>The MAC Address associated with the internal bridge-router interface (IBRI).</td>
</tr>
<tr>
<td>Routing VLANs</td>
<td>The same MAC Address is used by all VLAN routing interfaces. It will be</td>
</tr>
<tr>
<td></td>
<td>displayed above the per-VLAN information.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The identifier of the VLAN.</td>
</tr>
<tr>
<td>Logical Interface</td>
<td>The logical slot/port associated with the VLAN routing interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address associated with this VLAN.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask that is associated with this VLAN.</td>
</tr>
</tbody>
</table>
5.6 Virtual Router Redundancy Protocol Commands

This section describes the commands you use to view and configure Virtual Router Redundancy Protocol (VRRP) and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

5.6.1 ip vrrp (Global Config)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router. This command enables VRRP (v2 or v3, whichever version is the configured version) and makes it operational. For information about how to enable VRRPv3, see “fhrp version vrrp v3” on page 562.

Default none
Format ip vrrp
Mode Global Config

5.6.1.1 no ip vrrp

Use this command in Global Config mode to disable the default administrative mode of VRRP on the router.

Format no ip vrrp
Mode Global Config

5.6.2 ip vrrp (Interface Config)

Use this command in Interface Config mode to create a virtual router associated with the interface or range of interfaces. The parameter vrid is the virtual router ID, which has an integer value range from 1 to 255.

Format ip vrrp vrid
Mode Interface Config

5.6.2.1 no ip vrrp

Use this command in Interface Config mode to delete the virtual router associated with the interface. The virtual Router ID, vrid, is an integer value that ranges from 1 to 255.

Format no ip vrrp vrid
Mode Interface Config

5.6.3 ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter vrid is the virtual router ID which has an integer value ranging from 1 to 255.

Default disabled
Format ip vrrp vrid mode
Mode Interface Config
5.6.3.1  no ip vrrp mode
This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

**Format**  
`no ip vrrp vrid mode`

**Mode**  
Interface Config

5.6.4  ip vrrp ip
This command sets the virtual router IP address value for an interface or range of interfaces. The value for `ipaddr` is the IP address which is to be configured on that interface for VRRP. The parameter `vrid` is the virtual router ID which has an integer value range from 1 to 255. You can use the optional `[secondary]` parameter to designate the IP address as a secondary IP address.

**Default**  
`none`

**Format**  
`ip vrrp vrid ip ipaddr [secondary]`

**Mode**  
Interface Config

5.6.4.1  no ip vrrp ip
Use this command in Interface Config mode to delete a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

**Format**  
`no ip vrrp vrid ipaddress secondary`

**Mode**  
Interface Config

5.6.5  ip vrrp accept-mode
Use this command to allow the VRRP Master to accept ping packets sent to one of the virtual router’s IP addresses.

**Notice**  
VRRP accept-mode allows only ICMP Echo Request packets. No other type of packet is allowed to be delivered to a VRRP address.

**Default**  
`disabled`

**Format**  
`ip vrrp vrid accept-mode`

**Mode**  
Interface Config
5.6.5.1 no ip vrrp accept-mode
Use this command to prevent the VRRP Master from accepting ping packets sent to one of the virtual router’s IP addresses.

Format no ip vrrp vrid accept-mode
Mode Interface Config

5.6.6 ip vrrp authentication
This command sets the authorization details value for the virtual router configured on a specified interface or range of interfaces. The parameter {none | simple} specifies the authorization type for virtual router configured on the specified interface. The parameter [key] is optional, it is only required when authorization type is simple text password. The parameter vrid is the virtual router ID which has an integer value ranges from 1 to 255.

Default no authorization
Format ip vrrp vrid authentication {none | simple key}
Mode • Interface Config

5.6.6.1 no ip vrrp authentication
This command sets the default authorization details value for the virtual router configured on a specified interface or range of interfaces.

Format no ip vrrp vrid authentication
Mode • Interface Config

5.6.7 ip vrrp preempt
This command sets the preemption mode value for the virtual router configured on a specified interface or range of interfaces. The parameter vrid is the virtual router ID, which is an integer from 1 to 255.

Default enabled
Format ip vrrp vrid preempt
Mode • Interface Config

5.6.7.1 no ip vrrp preempt
This command sets the default preemption mode value for the virtual router configured on a specified interface or range of interfaces.

Format no ip vrrp vrid preempt
Mode • Interface Config
5.6.8 ip vrrp priority
This command sets the priority of a router within a VRRP group. It can be used to configure an interface or a range of interfaces. Higher values equal higher priority. The range is from 1 to 254. The parameter \texttt{vrid} is the virtual router ID, whose range is from 1 to 255.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the “address owner.” The priority of the address owner is always 255 so that the address owner is always master. If the master has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the master’s priority, the router will take over as master only if pre-empt mode is enabled.

**Default**: 100 unless the router is the address owner, in which case its priority is automatically set to 255.

**Format**: \texttt{ip vrrp vrid priority 1-254}

**Mode**: Interface Config

5.6.8.1 no ip vrrp priority
This command sets the default priority value for the virtual router configured on a specified interface or range of interfaces.

**Format**: \texttt{no ip vrrp vrid priority}

**Mode**: Interface Config

5.6.9 ip vrrp timers advertise
This command sets the frequency, in seconds, that an interface or range of interfaces on the specified virtual router sends a virtual router advertisement.

**Default**: 1

**Format**: \texttt{ip vrrp vrid timers advertise 1-255}

**Mode**: Interface Config

5.6.9.1 no ip vrrp timers advertise
This command sets the default virtual router advertisement value for an interface or range of interfaces.

**Format**: \texttt{no ip vrrp vrid timers advertise}

**Mode**: Interface Config

5.6.10 ip vrrp track interface
Use this command to alter the priority of the VRRP router based on the availability of its interfaces. This command is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if the IP on that interface is up. Otherwise, the tracked interface is down. You can use this command to configure a single interface or range of interfaces. The argument \texttt{slot/port} corresponds to a physical routing interface or VLAN routing interface. The keyword \texttt{vlan} is used to specify the VLAN ID of the routing VLAN directly instead of in a \texttt{slot/port} format.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the \texttt{priority} argument. When the interface is up for IP protocol, the priority will be incremented by the \texttt{priority} value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed interface. The default priority decrement is changed using the \texttt{priority} argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10.
5.6.10.1  no ip vrrp track interface

Use this command to remove the interface or range of interfaces from the tracked list or to restore the priority decrement to its default.

Format  no ip vrrp vrid track interface {slot/port|vlan 1-4093} [decrement]
Mode     Interface Config

5.6.11  ip vrrp track ip route

Use this command to track the route reachability on an interface or range of interfaces. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the `priority` argument. When the tracked route is added, the priority will be incremented by the same.

A VRRP configured interface can track more than one route. When a tracked route goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed route. By default no routes are tracked. If you specify just the route to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10. The default priority decrement is changed using the `priority` argument.

Default  priority: 10
Format    ip vrrp vrid track ip route ip-address/prefix-length [decrement priority]
Mode      Interface Config

5.6.11.1  no ip vrrp track ip route

Use this command to remove the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, the priority should be incremented by the decrement value if the route is not reachable.

Format    no ip vrrp vrid track interface slot/port [decrement]
Mode      Interface Config

5.6.12  show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format.

Format    show ip vrrp interface stats {slot/port|vlan 1-4093} vrid
Modes     •  Privileged EXEC
          •  User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>The time that the virtual router has been up, in days, hours, minutes and seconds.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol configured on the interface.</td>
</tr>
<tr>
<td>State Transitioned to Master</td>
<td>The total number of times virtual router state has changed to MASTER.</td>
</tr>
<tr>
<td>Advertisement Received</td>
<td>The total number of VRRP advertisements received by this virtual router.</td>
</tr>
</tbody>
</table>
5.6.13 show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring. This command takes no options.

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip vrrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modes</td>
<td>Privileged EXEC, User EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisement Interval Errors</td>
<td>The total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.</td>
</tr>
<tr>
<td>Authentication Failure</td>
<td>The total number of VRRP packets received that don't pass the authentication check.</td>
</tr>
<tr>
<td>IP TTL errors</td>
<td>The total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.</td>
</tr>
<tr>
<td>Zero Priority Packets Received</td>
<td>The total number of VRRP packets received by virtual router with a priority of '0'.</td>
</tr>
<tr>
<td>Zero Priority Packets Sent</td>
<td>The total number of VRRP packets sent by the virtual router with a priority of '0'.</td>
</tr>
<tr>
<td>Invalid Type Packets Received</td>
<td>The total number of VRRP packets received by the virtual router with invalid 'type' field.</td>
</tr>
<tr>
<td>Address List Errors</td>
<td>The total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.</td>
</tr>
<tr>
<td>Invalid Authentication Type</td>
<td>The total number of VRRP packets received with unknown authentication type.</td>
</tr>
<tr>
<td>Authentication Type Mismatch</td>
<td>The total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.</td>
</tr>
<tr>
<td>Packet Length Errors</td>
<td>The total number of VRRP packets received with packet length less than length of VRRP header.</td>
</tr>
</tbody>
</table>

5.6.14 show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is the VLAN ID of the routing VLAN instead of in a slot/port format. Use the output of the command to verify the track interface and track IP route configurations.

| Format | show ip vrrp interface {slot/port|vlan 1-4093} vrid |
|---|---|
| Modes | Privileged EXEC, User EXEC |

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The configured IP address for the Virtual router.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

`show ip vrrp interface <u/s/p> vrid`

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMAC address</td>
<td>The VMAC address of the specified router.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>The authentication type for the specific virtual router.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority value for the specific virtual router, taking into account any priority decrements for tracked interfaces or routes.</td>
</tr>
<tr>
<td>Configured Priority</td>
<td>The priority configured through the <code>ip vrrp vrid priority 1-254</code> command.</td>
</tr>
<tr>
<td>Advertisement interval</td>
<td>The advertisement interval in seconds for the specific virtual router.</td>
</tr>
<tr>
<td>Pre-Empt Mode</td>
<td>The preemption mode configured on the specified virtual router.</td>
</tr>
<tr>
<td>Administrative Mode</td>
<td>The status (Enable or Disable) of the specific router.</td>
</tr>
<tr>
<td>Accept Mode</td>
<td>When enabled, the VRRP Master can accept ping packets sent to one of the virtual router’s IP addresses.</td>
</tr>
<tr>
<td>State</td>
<td>The state (Master/backup) of the virtual router.</td>
</tr>
</tbody>
</table>

5.6.15 `show ip vrrp interface brief`

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format: `show ip vrrp interface brief`

Modes
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td><code>slot/port</code></td>
</tr>
<tr>
<td>VRID</td>
<td>The router ID of the virtual router.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The virtual router IP address.</td>
</tr>
<tr>
<td>Mode</td>
<td>Indicates whether the virtual router is enabled or disabled.</td>
</tr>
<tr>
<td>State</td>
<td>The state (Master/backup) of the virtual router.</td>
</tr>
</tbody>
</table>
5.7 VRRPv3 Commands

VRRPv3 provides address redundancy for both IPv4 and IPv6 router addresses. VRRPv3 support in FASTPATH is similar to VRRP support. The following table provides a summary of the differences.

<table>
<thead>
<tr>
<th>VRRPv2</th>
<th>VRRPv3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports redundancy to IPv4 addresses</td>
<td>Supports redundancy to IPv4 and IPv6 addresses</td>
</tr>
<tr>
<td>Supports authentication</td>
<td>Does not support authentication</td>
</tr>
<tr>
<td>No concept of link-local address in IPv4 address space</td>
<td>For IPv6 addresses, VRRP IP contains the link-local IPv6 address too.</td>
</tr>
<tr>
<td>The interval time used for sending VRRP Advertise-</td>
<td>The interval time is in the order of centiseconds.</td>
</tr>
<tr>
<td>ment packets is in seconds.</td>
<td></td>
</tr>
<tr>
<td>VRRP MAC address format is 00-00-5E-00-01-{VRID}</td>
<td>VRRP MAC address format for IPv6 VR IP is 00-00-5E-00-02-{VRID}</td>
</tr>
<tr>
<td>SNMP MIB RFC according to 2787. The counters are 32-bit ones.</td>
<td>SNMP MIB RFC as per RFC 6527. The counters are 64-bit ones.</td>
</tr>
</tbody>
</table>

To enable VRRP on the device, use the `ip vrrp` command. See "ip vrrp (Global Config)" on page 555. This command enables VRRP (v2 or v3, whichever version is the configured version) and makes it operational.

A command is available to configure debugging for VRRP packets. For information, see "debug ip vrrp" on page 211.

5.7.1 fhrp version vrrp v3

To enable Virtual Router Redundancy Protocol version 3 (VRRPv3) configuration on a device, use the `fhrp version vrrp v3` command in global configuration mode.

When VRRPv3 is in use, VRRP version 2 (VRRPv2) is unavailable. If you invoke `no fhrp version vrrp v3`, VRRPv3 is disabled and VRRPv2 is enabled. Also, operational data is reset, and the VRRPv2 configuration is applied. The same guidelines apply when VRRPv2 is in use and the `no ip vrrp` command is issued.

- **Defaults**: Disabled
- **Format**: `fhrp version vrrp v3`
- **Mode**: Global Config

5.7.2 no fhrp version vrrp v3

Use this command to disable the VRRPv3 and enable VRRPv2 on the device.

- **Format**: `no fhrp version vrrp v3`
- **Mode**: Global Config

5.7.3 snmp-server enable traps vrrp

Use this command to enable the two SNMP traps defined in the VRRPv2 and VRRPv3 MIB standards.

- **Defaults**: Enabled
- **Format**: `snmp-server enable traps vrrp`
- **Mode**: Global Config
5.7.3.1  **no snmp-server enable traps vrrp**

Use this command to disable the two SNMP traps defined in the VRRPv2 and VRRPv3 MIB standards.

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>no snmp-server enable traps vrrp</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

5.7.4  **vrrp**

Use the `vrrp` command to create a VRRPv3 group and enter VRRPv3 group configuration mode.

| Format     | vrrp group-id address-family {ipv4 | ipv6} |
|------------|------------------------------------------|
| Mode       | Interface Config                        |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-id</td>
<td>Virtual router group number. The range is from 1 to 255.</td>
</tr>
<tr>
<td>address-family</td>
<td>Specifies the address-family for this VRRP group.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Specifies IPv6 address.</td>
</tr>
</tbody>
</table>

5.7.4.1  **no vrrp**

Use the `no vrrp` command to remove the specified VRRPv3 group. Before you can use this command, you must disable Virtual Router using the `shutdown` command in the appropriate VRRP Config mode.

| Format     | no vrrp group-id address-family {ipv4 | ipv6} |
|------------|------------------------------------------|
| Mode       | Interface Config                        |

5.7.5  **preempt**

Use this command to configure the device to take over as master virtual router for a VRRP group if it has higher priority than the current master virtual route.

<table>
<thead>
<tr>
<th>Default</th>
<th>Enabled with default delay value of 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>preempt [delay minimum centiseconds]</td>
</tr>
<tr>
<td>Mode</td>
<td>VRRPv3 Config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay minimum</td>
<td>Number of seconds that the device will delay before issuing an advertisement claiming master ownership. The default delay is 0 centiseconds. The valid range is 0–3600 centiseconds.</td>
</tr>
</tbody>
</table>
5.7.5.1  no preempt
Use this command to prevent device from taking over as master virtual router for a VRRP group if it has higher priority than the current master virtual route.

Format  no preempt [delay minimum centiseconds]
Mode    VRRPv3 Config

5.7.6  accept-mode
Use this command to control whether a virtual router in master state will accept packets addressed to the address owner’s virtual IP address as its own if it is not the virtual IP address owner.

Default  Disabled
Format    accept-mode
Mode      VRRPv3 Config

5.7.6.1  no accept-mode
Use this command to reset the accept mode to the default value.

Format    no accept-mode
Mode      VRRPv3 Config

5.7.7  priority
Use this command to set the priority level of the device within a VRRPv3 group. The priority level controls which device becomes the master virtual router.

Default  100
Format    priority Level
Mode      VRRPv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Priority of the device within the VRRP group. The range is from 1 to 254. The default is 100.</td>
</tr>
</tbody>
</table>
5.7.7.1 no priority
Use this command to reset the priority level of the device to the default value.

**Format**

priority

**Mode**
VRRPv3 Config

5.7.8 timers advertise
Use this command to configure the interval between successive advertisements by the master virtual router in a VRRP group. To restore the default value, use the no form of this command.

The advertisements being sent by the master virtual router communicate the advertisement interval, state, and priority of the current master virtual router. The VRRP **timers advertise** command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. VRRP backup routers learn timer values from the master router advertisements. The timers configured on the master router always override any other timer settings that are used for calculating the master down time interval on VRRP backup routers.

**Default**
100

**Format**

timers advertise *centiseconds*

**Mode**
VRRPv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>centiseconds</td>
<td>Time interval between successive advertisements by the master virtual router. The unit of the interval is in centiseconds. The valid range is 1 to 4095 centiseconds.</td>
</tr>
</tbody>
</table>

5.7.8.1 no timers advertise
Use this command to reset the advertisement interval of the device to the default value.

**Format**

no timers advertise

**Mode**
VRRPv3 Config

5.7.9 shutdown
Use the **shutdown** command to disable the VRRP group configuration.

**Format**

shutdown

**Mode**
VRRPv3 Config
5.7.9.1 no shutdown

Enter the no shutdown command to update the virtual router state after completing configuration.

**Format**
```
no shutdown
```

**Mode**
VRRPv3 Config

5.7.10 address

Use this command to set the primary or secondary IP address of the device within a VRRPv3 group. To remove the secondary address, use the no form of this command.

If the primary or secondary option is not specified, the specified IP address is set as the primary. The Virtual IPv6 primary address should be a link-local address only. When a global IPv6 address is given as a primary address for the VRRP IP then the config fails with the following error message – “Error! Primary virtual IPv6 address should be a link-local address only.” Also the removing of the primary virtual IP (IPv4 or IPv6) is not allowed. The primary virtual IP of a virtual router can only be modified. The secondary virtual IP can be removed using the no form of the this command. Also, VRRPv3 for IPv6 requires that a primary virtual link-local IPv6 address is configured to allow the group to operate. After the primary link-local IPv6 address is established on the group, you can add the secondary global addresses.

**Format**
```
address ip-address [primary | secondary]
```

**Mode**
VRRPv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IPv4 or IPv6 address, it can be specified in one of the following format: ipv4-address, ipv6-link-local-address, ipv6-address/%prefix-len.</td>
</tr>
<tr>
<td>primary</td>
<td>(Optional) Set primary IP address of the VRRPv3 group.</td>
</tr>
<tr>
<td>secondary</td>
<td>(Optional) Set additional IP address of the VRRPv3 group.</td>
</tr>
</tbody>
</table>

5.7.10.1 no address

Use this command to remove the configured secondary IP or IPv6 address. The primary address can only be modified, not removed.

**Format**
```
no address ip-address secondary
```

**Mode**
VRRPv3 Config

5.7.11 track interface

Use this command to configure tracking of the interface for the device within a VRRPv3 group. Once interface tracking is configured, the VRRPv3 feature receives notifications when the interface changes state. The decrement option can be set to decrease the priority of the device within a VRRPv3 group by the specified value when the interface goes down.

**Default**
Enabled

**Format**
```
track interface {unit/slot/port | vlan vlan-id} [decrement number]
```

**Mode**
VRRPv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit/slot/port</td>
<td>The interface to track.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>The VLAN to track.</td>
</tr>
<tr>
<td>decrement</td>
<td>(Optional) Specify the VRRP priority decrement for the tracked object. The number is the amount by which priority is decremented. The range is 1–254.</td>
</tr>
<tr>
<td>number</td>
<td></td>
</tr>
</tbody>
</table>
5.7.11.1 no track interface
Use this command to disable tracking of the interface for the device within a VRRPv3 group.

Default: Enabled
Format: track interface {unit/slot/port | vlan vlan-id} [decrement number]
Mode: VRRPv3 Config

5.7.12 track ip route
Use this command to configure tracking of the IP route for the device within a Virtual Router Redundancy Protocol (VRRPv3) group. Once IP route tracking is configured, the VRRPv3 feature receives notifications when IP route changes state. The decrement option can be set to decrease the priority of the device within a VRRPv3 group by the specified value when the route becomes unavailable.

Default: Disabled
Format: track ip route ip-address/prefix-len [decrement number]
Mode: VRRPv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address/prefix-len</td>
<td>Prefix and prefix length of the route to be tracked.</td>
</tr>
<tr>
<td>decrement number</td>
<td>(Optional) Specify the VRRP priority decrement for the tracked route. The number is the amount by which priority is decremented. The range is 1–254.</td>
</tr>
</tbody>
</table>

5.7.12.1 no track ip route
Use this command to disable object tracking.

Format: no track ip route ip-address/prefix-len [decrement number]
Mode: VRRPv3 Config

5.7.13 clear vrrp statistics
Use this command to clear VRRP statistical information for given interface of the device within a VRRPv3 group and IP address family. If this command is issued without the optional arguments then the global statistics and all virtual routers (both IPv4 and IPv6) are reset.

If the optional arguments are specified, the statistics are reset for the virtual router corresponding to the given (IP address family, interface and VR-id) combination.

Format: clear vrrp statistics [{ipv4 | ipv6} {unit/slot/port | vlan vlan-id} vrid]
Mode: Privileged Exec

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) indicates the Virtual router group belongs to IPv4 address family.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) indicates the Virtual router group belongs to IPv6 address family.</td>
</tr>
<tr>
<td>unit/slot/port</td>
<td>(Optional) indicates the interface number to which the Virtual router belongs.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>(Optional) indicates the VLAN number to which the Virtual router belongs.</td>
</tr>
<tr>
<td>vrid</td>
<td>(Optional) Virtual router group number. The range is from 1 to 255.</td>
</tr>
</tbody>
</table>
5.7.14 show vrrp

This command displays information for all active VRRPv3 groups (no optional parameters), all active VRRPv3 groups configured in an IPv4 or IPv6 address family, or the active VRRPv3 groups configured in an IPv4 or IPv6 address family for the specified interface.

**Format**

```
show vrrp [(ipv4 | ipv6)] [(unit/slot/port | vlan vlan-id) vr-id]
```

**Mode**

Privileged Exec

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) indicates the Virtual router group belongs to IPv4 address family.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) indicates the Virtual router group belongs to IPv6 address family.</td>
</tr>
<tr>
<td>unit/slot/port</td>
<td>(Optional) indicates the interface number to which the Virtual router belongs.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>(Optional) indicates the VLAN number to which the Virtual router belongs.</td>
</tr>
<tr>
<td>vr-id</td>
<td>(Optional) Virtual router group number. The range is from 1 to 255.</td>
</tr>
</tbody>
</table>

**Example:** This example shows command output when no parameters are specified.

(Routing)#show vrrp

Admin Mode ....................................... Enable

1/0/2 - VRID 1 - Address-Family IPv4

Virtual IP address .................. 1.1.1.9
Secondary IP Address(es) .......... 1.1.1.4
........................................ 1.1.1.5
........................................ 1.1.1.6
Virtual MAC Address .............. 00:00:5e:00:01:01
Priority .................................. 0
Configured Priority ................. 111
Advertisement Interval .......... 120 centisec
Pre-empt Mode ....................... Enable
Accept Mode ......................... Enable
Administrative Mode ................. Enable
State ................................... Initialized
Master Router IP / Priority .... 1.1.1.3 (local) / 100
Master Advertisement interval ... 120 centisec
Master Down interval ............... 360 centisec

Track Interface State DecrementPriority
----------------------------------------
1/0/9 Down 222

Track Route(pfx/len) Reachable DecrementPriority
-------------------------------------

1/0/3 - VRID 2 - Address-Family IPv4

Virtual IP address .................. 3.3.2.9
Secondary IP Address(es) .......... 3.3.2.4
........................................ 3.3.2.5
........................................ 3.3.2.6
Virtual MAC Address .............. 00:00:5e:00:01:06
Priority .................................. 0
Configured Priority ................. 130
Advertisement Interval .......... 120 centisec
Pre-empt Mode ....................... Enable
Accept Mode.......................... Enable
Administrative Mode.................. Enable
State.................................. Initialized
Master Router IP / Priority........... 1.1.1.3 (local) / 100
Master Advertisement interval...... 120 centisec
Master Down interval............... 360 centisec

<table>
<thead>
<tr>
<th>Track Interface</th>
<th>State</th>
<th>DecrementPriority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/7</td>
<td>Down</td>
<td>125</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Track Route</th>
<th>Reachable</th>
<th>DecrementPriority</th>
</tr>
</thead>
</table>

1/0/12 - VRID 3 - Address-Family IPv6

Virtual IP address.................. 4001::2
Secondary IP Address(es)............ 4001::5
.................................... 4001::6
.................................... 4001::7
Virtual MAC Address.................. 00:00:5e:00:01:06
Priority................................ 0
Configured Priority.................. 130
Advertisement Interval................ 120 centisec
Pre-empt Mode......................... Enable
Accept Mode.......................... Enable
Administrative Mode.................. Enable
State.................................. Initialized
Master Router IP / Priority........... 4001::3 (local) / 100
Master Advertisement interval...... 120 centisec
Master Down interval............... 360 centisec

<table>
<thead>
<tr>
<th>Track Interface</th>
<th>State</th>
<th>DecrementPriority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/2</td>
<td>Down</td>
<td>250</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Track Route</th>
<th>Reachable</th>
<th>DecrementPriority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4004::3/32</td>
<td>True</td>
<td>20</td>
</tr>
</tbody>
</table>

**Example:** This example shows command output when the IPv4 parameter is specified.

(Routing)#show vrrp ipv4

Admin Mode.......................... Enable

1/0/2 - VRID 1 - Address-Family IPv4

Virtual IP address.................. 1.1.1.9
Secondary IP Address(es)............ 1.1.1.4
.................................... 1.1.1.5
.................................... 1.1.1.6
Virtual MAC Address.................. 00:00:5e:00:01:01
Priority................................ 0
Configured Priority.................. 111
Advertisement Interval................ 120 centisec
Pre-empt Mode......................... Enable
Accept Mode.......................... Enable
Administrative Mode.................. Enable
State.................................. Initialized
Master Router IP / Priority........... 1.1.1.3 (local) / 100
Master Advertisement interval...... 120 centisec
Master Down interval............... 360 centisec
Track Interface State DecrementPriority
------------------------  ------  ------------------------
1/0/7                  Down  125

Track Route(pfx/len)  Reachable DecrementPriority
------------------------  ------------  ------------------------

1/0/2 - VRID 1 - Address-Family IPv6

Virtual IP address......................... 1001::8
Secondary IP Address(es)............... 1001::5
............................................... 1001::6
............................................... 1001::7
Virtual MAC Address......................... 00:00:5e:00:01:01
Priority......................................... 0
Configured Priority........................ 100
Advertisement Interval.................... 100 centisec
Pre-empt Mode............................... Enable
Accept Mode.................................... Enable
Administrative Mode........................ Enable
State............................................. Initialized
Master Router IP / Priority............... 1001:1 (local) / 100
Master Advertisement interval.............. 100 centisec
Master Down interval....................... 300 centisec

Example: This example shows command output when the IPv6 parameter is specified.
(Routing)#show vrrp ipv6

Admin Mode................................. Enable

1/0/2 - VRID 1 - Address-Family IPv6

Virtual IP address......................... 1001::8
Secondary IP Address(es)............... 1001::5
............................................... 1001::6
............................................... 1001::7
Virtual MAC Address......................... 00:00:5e:00:01:01
Priority......................................... 0
Configured Priority........................ 100
Advertisement Interval.................... 100 centisec
Pre-empt Mode............................... Enable
Accept Mode.................................... Enable
Administrative Mode........................ Enable
State............................................. Initialized
Master Router IP / Priority............... 1001:1 (local) / 100
Master Advertisement interval.............. 100 centisec
Master Down interval....................... 300 centisec

Track Interface State DecrementPriority
------------------------  ------  ------------------------
1/0/9                  Down  222

Track Route(pfx/len)  Reachable DecrementPriority
------------------------  ------------  ------------------------
RES-PTP-POE CLI Reference Manual

---

**Track Route(pfx/len) Reachable Decrement Priority**

<table>
<thead>
<tr>
<th>pfx/len</th>
<th>Reachable</th>
<th>Decrement Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::2/32</td>
<td>True</td>
<td>14</td>
</tr>
</tbody>
</table>

1/0/12 - VRID 3 - Address-Family IPv6

Virtual IP address: 4001::2
Secondary IP Address(es): 4001::5
Secondary IP Address(es): 4001::6
Secondary IP Address(es): 4001::7
Virtual MAC Address: 00:00:5e:00:01:06
Priority: 130
Configured Priority: 130
Advertisement Interval: 120 centisec
Pre-empt Mode: Enable
Accept Mode: Enable
Administrative Mode: Enable
State: Master
Master Router IP / Priority: 4001::3 (local) / 130
Master Advertisement interval: 120 centisec
Master Down interval: 360 centisec

**Track Interface State Decrement Priority**

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Decrement Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/24</td>
<td>Down</td>
<td>320</td>
</tr>
</tbody>
</table>

**Track Route(pfx/len) Reachable Decrement Priority**

<table>
<thead>
<tr>
<th>pfx/len</th>
<th>Reachable</th>
<th>Decrement Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>7003::4/32</td>
<td>True</td>
<td>50</td>
</tr>
</tbody>
</table>

---

**Example:**

```
(Routing)#show vrrp ipv4 1/0/3 1
```

Virtual IP address: 1.1.1.9
Secondary IP Address(es): 1.1.1.4
Secondary IP Address(es): 1.1.1.5
Secondary IP Address(es): 1.1.1.6
Virtual MAC Address: 00:00:5e:00:01:01
Priority: 0
Configured Priority: 111
Advertisement Interval: 222 centisec
Pre-empt Mode: Enable
Accept Mode: Enable
Administrative Mode: Enable
State: Initialized
Master Router IP / Priority: 1.1.1.3 (local) / 100
Master Advertisement interval: 1000 centisec
Master Down interval: 3000 centisec

**Track Interface State Decrement Priority**

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Decrement Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/9</td>
<td>Down</td>
<td>222</td>
</tr>
</tbody>
</table>

**Track Route(pfx/len) Reachable Decrement Priority**

<table>
<thead>
<tr>
<th>pfx/len</th>
<th>Reachable</th>
<th>Decrement Priority</th>
</tr>
</thead>
</table>
5.7.15  show vrrp brief
This command displays brief information for all active VRRPv3 groups.

**Format**
```
show vrrp brief
```

**Mode**
Privileged Exec

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface on which VRRP is configured.</td>
</tr>
<tr>
<td>VRID</td>
<td>ID of the virtual router.</td>
</tr>
<tr>
<td>A-F</td>
<td>IP address family type (IPv4 or IPv6) this Virtual Router belongs to.</td>
</tr>
<tr>
<td>Pri</td>
<td>Priority range of the virtual router.</td>
</tr>
<tr>
<td>AdvIntvl</td>
<td>Advertisement interval configured for this virtual router.</td>
</tr>
<tr>
<td>Pre</td>
<td>Preemption state of the virtual router.</td>
</tr>
<tr>
<td>Acc</td>
<td>Accept Mode of the virtual router.</td>
</tr>
<tr>
<td>State</td>
<td>VRRP group state. The state can be one of the following: Init, Backup, Master</td>
</tr>
<tr>
<td>VR IP address</td>
<td>Virtual IP address for a VRRP group.</td>
</tr>
</tbody>
</table>

**Example:**
(Routing)# show vrrp brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>VRID</th>
<th>A-F</th>
<th>Pri</th>
<th>AdvIntvl</th>
<th>Pre</th>
<th>Acc</th>
<th>State</th>
<th>VR IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>1</td>
<td>IPv4</td>
<td>100</td>
<td>200s</td>
<td>Y</td>
<td>Y</td>
<td>Init</td>
<td>192.0.1.10</td>
</tr>
<tr>
<td>0/3</td>
<td>2</td>
<td>IPv4</td>
<td>200</td>
<td>200s</td>
<td>Y</td>
<td>Y</td>
<td>Init</td>
<td>124.0.3.17</td>
</tr>
<tr>
<td>0/1</td>
<td>7</td>
<td>IPv6</td>
<td>100</td>
<td>200s</td>
<td>Y</td>
<td>Y</td>
<td>Backup</td>
<td>5002::1</td>
</tr>
<tr>
<td>0/5</td>
<td>2</td>
<td>IPv6</td>
<td>20</td>
<td>200s</td>
<td>Y</td>
<td>Y</td>
<td>Master</td>
<td>2001::2</td>
</tr>
</tbody>
</table>

5.7.16  show vrrp statistics
This command displays statistical information for a given VRRPv3 group or displays the global statistics. If this command is issued without the optional arguments then the global statistics are displayed.

If the optional arguments are specified, the statistics are displayed for the virtual router corresponding to the given (IP address family, interface and VR-id) combination.

**Format**
```
show vrrp statistics {{ipv4|ipv6} {unit/slot/port | vlan vlan-id} vrid]
```

**Mode**
Privileged Exec

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) indicates the Virtual router group belongs to IPv4 address family.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) indicates the Virtual router group belongs to IPv6 address family.</td>
</tr>
<tr>
<td>unit/slot/port</td>
<td>(Optional) indicates the interface number to which the Virtual router belongs.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>(Optional) indicates the VLAN number to which the Virtual router belongs.</td>
</tr>
<tr>
<td>vr-id</td>
<td>(Optional) Virtual router group number. The range is from 1 to 255.</td>
</tr>
</tbody>
</table>
Example:

(Routing)# show vrrp statistics ipv6 1/0/1 2

Master Transitions............................ 2
New Master Reason.......................... Priority
Advertisements Received.................... 64
Advertisements Sent........................ 12
Advertisement Interval Errors............... 0
IP TTL Errors................................. 1
Last Protocol Error Reason.................. Version Error
Zero Priority Packets Received............... 0
Zero Priority Packets Sent................... 1
Invalid Type Packets Received............... 0
Address List Errors........................ 2
Packet Length Errors........................ 4
Row Discontinuity Time...................... 0 days 0 hrs 0 mins 0 secs
Refresh Rate (in milliseconds)............. 0

(Routing)# show vrrp statistics

Router Checksum Errors..................... 2
Router Version Errors...................... 3
Router VRID Errors........................ 4
Global Statistics Discontinuity Time........ 0 days 0 hrs 0 mins 0 secs

5.8 DHCP and BOOTP Relay Commands

This section describes the commands you use to configure BootP/DHCP Relay on the switch. A DHCP relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

5.8.1 bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Default  disabled
Format    bootpdhcprelay cidoptmode
Mode      • Global Config
          • Virtual Router Config
5.8.1.1  no bootpdhcprelay cidoptmode
This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

**Format**
```
no bootpdhcprelay cidoptmode
```

**Mode**
- Global Config
- Virtual Router Config

5.8.2  bootpdhcprelay maxhopcount
This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The `hops` parameter has a range of 1 to 16.

**Default**
4

**Format**
```
bootpdhcprelay maxhopcount 1-16
```

**Mode**
- Global Config
- Virtual Router Config

5.8.2.1  no bootpdhcprelay maxhopcount
This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

**Format**
```
no bootpdhcprelay maxhopcount
```

**Mode**
- Global Config
- Virtual Router Config

5.8.3  bootpdhcprelay minwaittime
This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

**Default**
0

**Format**
```
bootpdhcprelay minwaittime 0-100
```

**Mode**
- Global Config
- Virtual Router Config
5.8.3.1  no bootpdhcprelay minwaittime
This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

Format  no bootpdhcprelay minwaittime
Mode    • Global Config
         • Virtual Router Config

5.8.4    bootpdhcprelay serverip
This command configures the server IP address of the BootP/DHCP Relay on the system. The ipaddr parameter is the IP address of the server.

Default  0.0.0.0
Format    bootpdhcprelay serverip ipaddr
Mode      Global Config

5.8.4.1  no bootpdhcprelay serverip
This command returns the server IP address of the BootP/DHCP Relay on the system to the default value of 0.0.0.0.

Format    no bootpdhcprelay serverip
Mode      Global Config

5.8.5    bootpdhcprelay enable
Use this command to enable the relay of DHCP packets.

Default  disabled
Format    bootpdhcprelay enable
Mode      Global Config
5.8.5.1 no bootpdhcprelay enable

Use this command to disable the relay of DHCP packets.

Default disabled

Format no bootpdhcprelay enable

Mode Global Config

5.8.6 show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format show bootpdhcprelay

Modes

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Hop Count</td>
<td>The maximum allowable relay agent hops.</td>
</tr>
<tr>
<td>Minimum Wait Time (Seconds)</td>
<td>The minimum wait time.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>Indicates whether relaying of requests is enabled or disabled.</td>
</tr>
<tr>
<td>Circuit Id Option Mode</td>
<td>The DHCP circuit Id option which may be enabled or disabled.</td>
</tr>
</tbody>
</table>

5.8.7 show ip bootpdhcprelay

This command displays BootP/DHCP Relay information.

Format show ip bootpdhcprelay

Modes

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Hop Count</td>
<td>The maximum allowable relay agent hops.</td>
</tr>
<tr>
<td>Minimum Wait Time (Seconds)</td>
<td>The minimum wait time.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>Indicates whether relaying of requests is enabled or disabled.</td>
</tr>
<tr>
<td>Circuit Id Option Mode</td>
<td>The DHCP circuit Id option which may be enabled or disabled.</td>
</tr>
</tbody>
</table>

**Example:** The following shows an example of the command.

(Routing) > show ip bootpdhcprelay

Maximum Hop Count......................... 4
Minimum Wait Time(Seconds).................. 0
Admin Mode................................ Disable
Circuit Id Option Mode..................... Enable
5.9 IP Helper Commands
This section describes the commands to configure and monitor the IP Helper agent. IP Helper relays DHCP and other broadcast UDP packets from a local client to one or more servers which are not on the same network at the client.

The IP Helper feature provides a mechanism that allows a router to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications to reach servers on nonlocal subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

The network administrator can configure relay entries both globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). The network administrator may configure multiple relay entries for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. That is, if a packet’s destination UDP port matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

The network administrator can configure discard relay entries, which direct the system to discard matching packets. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

In addition to configuring the server addresses, the network administrator also configures which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI as a convenience, but the network administrator can configure a relay entry with any UDP port number. The network administrator may configure relay entries that do not specify a destination UDP port. The relay agent relays assumes these entries match packets with the UDP destination ports listed in Table 10. This is the list of default ports.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>UDP Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEN–116 Name Service</td>
<td>42</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
</tr>
<tr>
<td>NetBIOS Name Server</td>
<td>137</td>
</tr>
<tr>
<td>NetBIOS Datagram Server</td>
<td>138</td>
</tr>
<tr>
<td>TACACS Server</td>
<td>49</td>
</tr>
<tr>
<td>Time Service</td>
<td>37</td>
</tr>
<tr>
<td>DHCP</td>
<td>67</td>
</tr>
<tr>
<td>Trivial File Transfer Protocol (TFTP)</td>
<td>69</td>
</tr>
</tbody>
</table>

The system limits the number of relay entries to four times the maximum number of routing interfaces. The network administrator can allocate the relay entries as he likes. There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for a given {interface, UDP port} pair.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays to the client packets that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent checks if the interface is configured to relay the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent checks if there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed. Note that if the packet matches a discard relay entry on the ingress interface, then the packet is not forwarded, regardless of the global configuration.
The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF).
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

5.9.1 clear ip helper statistics

Use this command to reset to zero the statistics displayed in the `show ip helper statistics` command.

**Format**
```
clear ip helper statistics
```

**Mode**
Privileged EXEC

**Example:** The following shows an example of the command.
```
(switch) #clear ip helper statistics
```

5.9.2 ip helper-address (Global Config)

Use this command to configure the relay of certain UDP broadcast packets received on any interface. This command can be invoked multiple times, either to specify multiple server addresses for a given UDP port number or to specify multiple UDP port numbers handled by a specific server.

**Default**
No helper addresses are configured.

**Format**
```
ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]
```

**Mode**
- Global Config
- Virtual Router Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server-address</td>
<td>The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.</td>
</tr>
<tr>
<td>dest-udp-port</td>
<td>A destination UDP port number from 0 to 65535.</td>
</tr>
</tbody>
</table>
Example: To relay DHCP packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands:

```
(switch)#config
(switch)(config)#ip helper-address 10.1.1.1 dhcp
(switch)(config)#ip helper-address 10.1.2.1 dhcp
```

Example: To relay UDP packets received on any interface for all default ports to the server at 20.1.1.1, use the following commands:

```
(switch)#config
(switch)(config)#ip helper-address 20.1.1.1
```

5.9.2.1 no ip helper-address (Global Config)

Use the no form of the command to delete an IP helper entry. The command no ip helper-address with no arguments clears all global IP helper addresses.

**Format**

```
no ip helper-address [server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]
```

**Mode**

Global Config

5.9.3 ip helper-address (Interface Config)

Use this command to configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

**Default**

No helper addresses are configured.

**Format**

```
ip helper-address {server-address | discard} [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]
```

**Mode**

Interface Config
Example: To relay DHCP packets received on interface 0/2 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands:

```
(switch)#config
(switch)(config)#interface 0/2
(switch)(interface 0/2)#ip helper-address 192.168.10.1 dhcp
(switch)(interface 0/2)#ip helper-address 192.168.20.1 dhcp
```

Example: To relay both DHCP and DNS packets to 192.168.30.1, use the following commands:

```
(switch)#config
(switch)(config)#interface 0/2
(switch)(interface 0/2)#ip helper-address 192.168.30.1 dhcp
(switch)(interface 0/2)#ip helper-address 192.168.30.1 dns
```

Example: This command takes precedence over an ip helper-address command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than 0/2 and 0/17 to 192.168.40.1, relays DHCP and DNS packets received on 0/2 to 192.168.40.2, relays SNMP traps (port 162) received on interface 0/17 to 192.168.23.1, and drops DHCP packets received on 0/17:

```
(switch)#config
(switch)(config)#ip helper-address 192.168.40.1 dhcp
(switch)(config)#interface 0/2
(switch)(interface 0/2)#ip helper-address 192.168.40.2 dhcp
(switch)(interface 0/2)#ip helper-address 192.168.40.2 domain
(switch)(interface 0/2)#exit
(switch)(config)#interface 0/17
(switch)(interface 0/17)#ip helper-address 192.168.23.1 162
(switch)(interface 0/17)#ip helper-address discard dhcp
```
5.9.3.1 no ip helper-address (Interface Config)
Use this command to delete a relay entry on an interface. The no command with no arguments clears all helper addresses on the interface.

Format
no ip helper-address [server-address | discard ]?[dest-udp-port | dhcp | domain |
isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip |
tacacs | tftp | time]

Mode
Interface Config

5.9.4 ip helper enable
Use this command to enable relay of UDP packets. This command can be used to temporarily disable IP helper without deleting all IP helper addresses. This command replaces the bootpdhcprelay enable command, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

Default
disabled

Format
ip helper enable

Mode
• Global Config
• Virtual Router Config

Example: The following shows an example of the command.
(switch)(config)#ip helper enable

5.9.4.1 no ip helper enable
Use the no form of this command to disable relay of all UDP packets.

Format
no ip helper enable

Mode
Global Config

5.9.5 show ip helper-address
Use this command to display the IP helper address configuration. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format.

Format
show ip helper-address [{slot/port|vlan 1-4093}]

Mode
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>The relay configuration is applied to packets that arrive on this interface. This field is set to any for global IP helper entries.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as any are applied to packets with the destination UDP ports listed in Table 4.</td>
</tr>
<tr>
<td>Discard</td>
<td>If Yes, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>The number of times the IP helper entry has been used to relay or discard a packet.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IPv4 address of the server to which packets are relayed.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

```
(switch) #show ip helper-address
```

IP helper is enabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>UDP Port</th>
<th>Discard</th>
<th>Hit Count</th>
<th>Server Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>dhcp</td>
<td>No</td>
<td>10</td>
<td>10.100.1.254</td>
</tr>
<tr>
<td>0/17</td>
<td>any</td>
<td>Yes</td>
<td>2</td>
<td>10.100.2.254</td>
</tr>
<tr>
<td>any</td>
<td>dhcp</td>
<td>No</td>
<td>0</td>
<td>10.200.1.254</td>
</tr>
</tbody>
</table>

5.9.6 **show ip helper statistics**

Use this command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent

**Format**  
show ip helper statistics

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP client messages received</td>
<td>The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL=1 and having valid source and destination IP addresses.</td>
</tr>
<tr>
<td>DHCP client messages relayed</td>
<td>The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.</td>
</tr>
<tr>
<td>DHCP server messages received</td>
<td>The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.</td>
</tr>
<tr>
<td>DHCP server messages relayed</td>
<td>The number of DHCP server messages relayed to a client.</td>
</tr>
<tr>
<td>UDP clients messages received</td>
<td>The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.</td>
</tr>
<tr>
<td>UDP clients messages relayed</td>
<td>The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.</td>
</tr>
<tr>
<td>DHCP message hop count exceeded max</td>
<td>The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.</td>
</tr>
<tr>
<td>DHCP message with secs field below min</td>
<td>The number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.</td>
</tr>
<tr>
<td>DHCP message with giaddr set to local address</td>
<td>The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent’s own IP addresses. In this case, another device is attempting to spoof the relay agent’s address. The relay agent does not relay such packets. A log message gives details for each occurrence.</td>
</tr>
<tr>
<td>Packets with expired TTL</td>
<td>The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.</td>
</tr>
<tr>
<td>Packets that matched a discard entry</td>
<td>The number of packets ignored by the relay agent because they match a discard relay entry.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.
(switch)#show ip helper statistics

DHCP client messages received .................. 8
DHCP client messages relayed ................. 2
DHCP server messages received ............... 2
DHCP server messages relayed ............... 2
UDP client messages received ............... 8
UDP client messages relayed ............... 2
DHCP message hop count exceeded max...... 0
DHCP message with secs field below min.... 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL .................... 0
Packets that matched a discard entry ...... 0

5.10 Open Shortest Path First Commands
This section describes the commands you use to view and configure Open Shortest Path First (OSPF), which is a link-state routing protocol that you use to route traffic within a network. This section contains the following subsections:
- “General OSPF Commands” on page 583
- “OSPF Interface Commands” on page 603
- “IP Event Dampening Commands” on page 609
- “OSPFv2 Stub Router Commands” on page 613
- “OSPF Show Commands” on page 614

General OSPF Commands

5.10.1 router ospf
Use this command to enter Router OSPF mode.

Format router ospf
Mode Global Config

5.10.2 enable (OSPF)
This command resets the default administrative mode of OSPF in the router (active).

Default enabled
Format enable
Mode Router OSPF Config
5.10.2.1 no enable (OSPF)
This command sets the administrative mode of OSPF in the router to inactive.

**Format**  
no enable

**Mode**  
Router OSPF Config

5.10.3 network area (OSPF)
Use this command to enable OSPFv2 on an interface and set its area ID if the IP address of an interface is covered by this network command.

**Default**  
disabled

**Format**  
network ip-address wildcard-mask area area-id

**Mode**  
Router OSPF Config

5.10.3.1 no network area (OSPF)
Use this command to disable the OSPFv2 on an interface if the IP address of an interface was earlier covered by this network command.

**Format**  
no network ip-address wildcard-mask area area-id

**Mode**  
Router OSPF Config

5.10.4 1583compatibility
This command enables OSPF 1583 compatibility.

**Notice**  
1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

**Default**  
enabled

**Format**  
1583compatibility

**Mode**  
Router OSPF Config
5.10.4.1 no 1583compatibility
This command disables OSPF 1583 compatibility.

Format: no 1583compatibility
Mode: Router OSPF Config

5.10.5 area default-cost (OSPF)
This command configures the default cost for the stub area. You must specify the area ID and an integer value between 1-16777215.

Format: area areaid default-cost 1-16777215
Mode: Router OSPF Config

5.10.6 area nssa (OSPF)
This command configures the specified areaid to function as an NSSA.

Format: area areaid nssa
Mode: Router OSPF Config

5.10.6.1 no area nssa
This command disables nssa from the specified area id.

Format: no area areaid nssa
Mode: Router OSPF Config

5.10.7 area nssa default-info-originate (OSPF)
This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is "***". The metric type can be comparable (nssa-external 1) or noncomparable (nssa-external 2).

Format: area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]
Mode: Router OSPF Config
5.10.7.1  no area nssa default-info-originate (OSPF)
This command disables the default route advertised into the NSSA.

**Format**
no area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]

**Mode**
Router OSPF Config

5.10.8  area nssa no-redistribute (OSPF)
This command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

**Format**
area areaid nssa no-redistribute

**Mode**
Router OSPF Config

5.10.8.1  no area nssa no-redistribute (OSPF)
This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

**Format**
no area areaid nssa no-redistribute

**Mode**
Router OSPF Config

5.10.9  area nssa no-summary (OSPF)
This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

**Format**
area areaid nssa no-summary

**Mode**
Router OSPF Config

5.10.9.1  no area nssa no-summary (OSPF)
This command disables nssa from the summary LSAs.

**Format**
no area areaid nssa no-summary

**Mode**
Router OSPF Config

5.10.10  area nssa translator-role (OSPF)
This command configures the translator role of the NSSA. A value of **always** causes the router to assume the role of the translator the instant it becomes a border router and a value of **candidate** causes the router to participate in the translator election process when it attains border router status.

**Format**
area areaid nssa translator-role {always | candidate}

**Mode**
Router OSPF Config
5.10.10  no area nssa translator-role (OSPF)
This command disables the nssa translator role from the specified area id.

**Format**
no area areaid nssa translator-role {always | candidate}

**Mode**
Router OSPF Config

5.10.11  area nssa translator-stab-intv (OSPF)
This command configures the translator stabilityinterval of the NSSA. The stabilityinterval is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

**Format**
area areaid nssa translator-stab-intv stabilityinterval

**Mode**
Router OSPF Config

5.10.11.1  no area nssa translator-stab-intv (OSPF)
This command disables the nssa translator's stabilityinterval from the specified area id.

**Format**
no area areaid nssa translator-stab-intv stabilityinterval

**Mode**
Router OSPF Config

5.10.12  area range (OSPF)
Use the area range command in Router Configuration mode to configure a summary prefix that an area border router advertises for a specific area.

**Default**
No area ranges are configured by default. No cost is configured by default.

**Format**
area areaid range ip-address netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost cost]

**Mode**
OSPFv2 Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>The area identifier for the area whose networks are to be summarized.</td>
</tr>
<tr>
<td>prefix netmask</td>
<td>The summary prefix to be advertised when the ABR computes a route to one or more networks within this prefix in this area.</td>
</tr>
<tr>
<td>summarylink</td>
<td>When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.</td>
</tr>
<tr>
<td>nssaexternallink</td>
<td>When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.</td>
</tr>
<tr>
<td>advertise</td>
<td>[Optional] When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.</td>
</tr>
<tr>
<td>not-advertise</td>
<td>[Optional] When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. When the not-advertise option is given, any static cost previously configured is removed from the system configuration.</td>
</tr>
</tbody>
</table>
5.10.12.1 no area range
The no form of this command deletes a specified area range or reverts an option to its default.

Format  no area areaid range prefix netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost]
Mode     OSPFv2 Router Configuration

Example: The following shows an example of the command.

!! Create area range.
(Router) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink
!! Delete area range.
(Router) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink

The no form may be used to revert the [advertise | not-advertise] option to its default without deleting the area range. Deleting and recreating the area range would cause OSPF to temporarily advertise the prefixes contained within the range. Note that using either the advertise or not-advertise keyword reverts the configuration to the default. For example:

!! Create area range. Suppress summary.
(Router) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink not-advertise
!! Advertise summary.
(Router) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink not-advertise

The no form may be used to remove a static area range cost, so that OSPF sets the cost to the largest cost among the contained routes.

!! Create area range with static cost.
(Router) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink cost 1000
!! Remove static cost.
(Router) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink cost

5.10.13 area stub (OSPF)
This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format  area areaid stub
Mode     Router OSPF Config
5.10.13.1 no area stub
This command deletes a stub area for the specified area ID.

Format  no area areaid stub
Mode    Router OSPF Config

5.10.14 area stub no-summary (OSPF)
This command configures the Summary LSA mode for the stub area identified by areaid. Use this command to prevent LSA Summaries from being sent.

Default  disabled
Format    area areaid stub no-summary
Mode      Router OSPF Config

5.10.14.1 no area stub no-summary
This command configures the default Summary LSA mode for the stub area identified by areaid.

Format  no area areaid stub no-summary
Mode    Router OSPF Config

5.10.15 area virtual-link (OSPF)
This command creates the OSPF virtual interface for the specified areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format  area areaid virtual-link neighbor
Mode    Router OSPF Config
5.10.15.1 no area virtual-link
This command deletes the OSPF virtual interface from the given interface, identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format: no area areaid virtual-link neighbor
Mode: Router OSPF Config

5.10.16 area virtual-link authentication
This command configures the authentication type and key for the OSPF virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor. The value for type is either none, simple, or encrypt. The key is composed of standard displayable, noncontrol keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id in the range of 0 and 255 must be specified. The default value for authentication type is none. Neither the default password key nor the default key id are configured.

Default: none
Format: area areaid virtual-link neighbor authentication {none | {simple key} | {encrypt key keyid}}
Mode: Router OSPF Config

5.10.16.1 no area virtual-link authentication
This command configures the default authentication type for the OSPF virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format: no area areaid virtual-link neighbor authentication
Mode: Router OSPF Config

5.10.17 area virtual-link dead-interval (OSPF)
This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

Default: 40
Format: area areaid virtual-link neighbor dead-interval seconds
Mode: Router OSPF Config
5.10.17.1 no area virtual-link dead-interval
This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor.

**Format**

no area areaid virtual-link neighbor dead-interval

**Mode**

Router OSPF Config

5.10.18 area virtual-link hello-interval (OSPF)
This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

**Default**

10

**Format**

area areaid virtual-link neighbor hello-interval 1-65535

**Mode**

Router OSPF Config

5.10.18.1 no area virtual-link hello-interval
This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor.

**Format**

no area areaid virtual-link neighbor hello-interval

**Mode**

Router OSPF Config

5.10.19 area virtual-link retransmit-interval (OSPF)
This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600.

**Default**

5

**Format**

area areaid virtual-link neighbor retransmit-interval seconds

**Mode**

Router OSPF Config
5.10.19.1 no area virtual-link retransmit-interval
This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format no area areaid virtual-link neighbor retransmit-interval
Mode Router OSPF Config

5.10.20 area virtual-link transmit-delay (OSPF)
This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600 (1 hour).

Default 1
Format area areaid virtual-link neighbor transmit-delay seconds
Mode Router OSPF Config

5.10.20.1 no area virtual-link transmit-delay
This command resets the default transmit delay for the OSPF virtual interface to the default value.

Format no area areaid virtual-link neighbor transmit-delay
Mode Router OSPF Config

5.10.21 auto-cost (OSPF)
By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the auto-cost reference bandwidth and bandwidth commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where interface bandwidth is defined by the bandwidth command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the auto-cost command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1-4294967 Mbps.

Default 100 Mbps
Format auto-cost reference-bandwidth 1-4294967
Mode Router OSPF Config
5.10.21.1 no auto-cost reference-bandwidth (OSPF)
Use this command to set the reference bandwidth to the default value.

**Format**
```
no auto-cost reference-bandwidth
```

**Mode**
Router OSPF Config

5.10.22 capability opaque
Use this command to enable Opaque Capability on the Router. The information contained in Opaque LSAs may be used directly by OSPF or indirectly by an application wishing to distribute information throughout the OSPF domain. FASTPATH supports the storing and flooding of Opaque LSAs of different scopes. The default value of enabled means that OSPF will forward opaque LSAs by default. If you want to upgrade from a previous release, where the default was disabled, opaque LSA forwarding will be enabled. If you want to disable opaque LSA forwarding, then you should enter the command no capability opaque in OSPF router configuration mode after the software upgrade.

**Default**
enabled

**Format**
capability opaque

**Mode**
Router Config

5.10.22.1 no capability opaque
Use this command to disable opaque capability on the router.

**Format**
```
no capability opaque
```

**Mode**
Router Config

5.10.23 clear ip ospf
Use this command to disable and re-enable OSPF for the specified virtual router. If no virtual router is specified, the default router is disabled and re-enabled.

**Format**
```
clear ip ospf [vrf vrf-name]
```

**Mode**
Privileged EXEC

5.10.24 clear ip ospf configuration
Use this command to reset the OSPF configuration to factory defaults for the specified virtual router. If no virtual router is specified, the default router is cleared.

**Format**
```
clear ip ospf configuration [vrf vrf-name]
```

**Mode**
Privileged EXEC

5.10.25 clear ip ospf counters
Use this command to reset global and interface statistics for the specified virtual router. If no virtual router is specified, the global and interface statistics are reset for the default router.

**Format**
```
clear ip ospf counters
```

**Mode**
Privileged EXEC
5.10.26  clear ip ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors for the specified virtual router. On each neighbor’s interface, send a one-way hello. Adjacencies may then be re-established. If no router is specified, adjacency with all OSPF neighbors is dropped for the default router. To drop all adjacencies with a specific router ID, specify the neighbor’s Router ID using the optional parameter [neighbor-id].

Format  clear ip ospf neighbor [ vrf vrf-name] [neighbor-id]
Mode     Privileged EXEC

5.10.27  clear ip ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter [slot/port]. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [neighbor-id].

Format  clear ip ospf neighbor interface [slot/port] [neighbor-id]
Mode     Privileged EXEC

5.10.28  clear ip ospf redistribution

Use this command to flush all self-originated external LSAs for the specified virtual router. If no router is specified, the command is executed for the default router. Reapply the redistribution configuration and reoriginate prefixes as necessary.

Format  clear ip ospf redistribution [vrf vrf-name]
Mode     Privileged EXEC
5.10.29  default-information originate (OSPF)
This command is used to control the advertisement of default routes.

Default  
  •  metric—unspecified
  •  type—2

Format  
  default-information originate [always] [metric 0-16777214] [metric-type {1 | 2}]

Mode  
  Router OSPF Config

5.10.29.1  no default-information originate (OSPF)
This command is used to control the advertisement of default routes.

Format  
  no default-information originate [metric] [metric-type]

Mode  
  Router OSPF Config

5.10.30  default-metric (OSPF)
This command is used to set a default for the metric of distributed routes.

Format  
  default-metric 1-16777214

Mode  
  Router OSPF Config

5.10.30.1  no default-metric (OSPF)
This command is used to set a default for the metric of distributed routes.

Format  
  no default-metric

Mode  
  Router OSPF Config

5.10.31  distance ospf (OSPF)
This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value. The range of preference value is 1 to 255.

Default  
  110

Format  
  distance ospf {intra-area 1-255 | inter-area 1-255 | external 1-255}

Mode  
  Router OSPF Config
5.10.31 no distance ospf
This command sets the default route preference value of OSPF routes in the router. The type of OSPF can be intra, inter, or external. All the external type routes are given the same preference value.

Format
no distance ospf {intra-area | inter-area | external}
Mode
Router OSPF Config

5.10.32 distribute-list out (OSPF)
Use this command to specify the access list to filter routes received from the source protocol.

Format
distribute-list 1-199 out {rip | static | connected}
Mode
Router OSPF Config

5.10.32.1 no distribute-list out
Use this command to specify the access list to filter routes received from the source protocol.

Format
no distribute-list 1-199 out {rip | static | connected}
Mode
Router OSPF Config

5.10.33 exit-overflow-interval (OSPF)
This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave overflow state until restarted. The range for seconds is 0 to 2147483647 seconds.

Default
0
Format
exit-overflow-interval seconds
Mode
Router OSPF Config
5.10.33.1 no exit-overflow-interval
This command configures the default exit overflow interval for OSPF.

**Format**
```
no exit-overflow-interval
```

**Mode**
Router OSPF Config

5.10.34 external-lsdb-limit (OSPF)
This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of nondefault AS-external-LSAs in a router’s link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit nondefault AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for limit is -1 to 2147483647.

**Default**
-1

**Format**
```
external-lsdb-limit limit
```

**Mode**
Router OSPF Config

5.10.34.1 no external-lsdb-limit
This command configures the default external LSDB limit for OSPF.

**Format**
```
no external-lsdb-limit
```

**Mode**
Router OSPF Config

5.10.35 log-adjacency-changes
To enable logging of OSPFv2 neighbor state changes, use the log-adjacency-changes command in router configuration mode. State changes are logged with INFORMATIONAL severity.

**Default**
Adjacency state changes are logged, but without the detail option.

**Format**
```
log-adjacency-changes [detail]
```

**Mode**
OSPFv2 Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) When this keyword is specified, all adjacency state changes are logged. Otherwise, OSPF only logs transitions to FULL state and when a backwards transition occurs.</td>
</tr>
</tbody>
</table>
5.10.35.1 no log-adjacency-changes
Use the no form of the command to disable state change logging.

Format no log-adjacency-changes [detail]
Mode OSPFv2 Router Configuration

5.10.36 prefix-suppression (Router OSPF Config)
This command suppresses the advertisement of all the IPv4 prefixes except for prefixes that are associated with secondary IPv4 addresses, loopbacks, and passive interfaces from the OSPFv2 router advertisements.
To suppress a loopback or passive interface, use the `ip ospf prefix-suppression` command in interface configuration mode. Prefixes associated with secondary IPv4 addresses can never be suppressed.

Default Prefix suppression is disabled.
Format prefix-suppression
Mode Router OSPF Config

5.10.36.1 no prefix-suppression
This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format no prefix-suppression
Mode Router OSPF Config

5.10.37 prefix-suppression (Router OSPFv3 Config)
This command suppresses the advertisement of all the IPv6 prefixes except for prefixes that are associated with secondary IPv6 addresses, loopbacks, and passive interfaces from the OSPFv3 router advertisements.
To suppress a loopback or passive interface, use the `ipv ospf prefix-suppression` command in interface configuration mode. Prefixes associated with secondary IPv6 addresses can never be suppressed.

Default Prefix suppression is disabled.
Format prefix-suppression
Mode Router OSPFv3 Config
5.10.37.1 no prefix-suppression
This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

**Format**
```
no prefix-suppression
```

**Mode**
Router OSPFv3 Config

5.10.38 router-id (OSPF)
This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The `ipaddress` is a configured value.

**Format**
```
router-id ipaddress
```

**Mode**
Router OSPF Config

5.10.39 redistribute (OSPF)
This command configures OSPF protocol to allow redistribution of routes from the specified source protocol/ routers.

**Default**
- metric—unspecified
- type—2
- tag—0

**Format**
```
redistribute {rip | static | connected} [metric 0-16777214] [metric-type {1 | 2}] [tag 0-4294967295] [subnets]
```

**Mode**
Router OSPF Config

5.10.39.1 no redistribute
This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/ routers.

**Format**
```
no redistribute {rip | static | connected} [metric] [metric-type] [tag] [subnets]
```

**Mode**
Router OSPF Config

5.10.40 maximum-paths (OSPF)
This command sets the number of paths that OSPF can report for a given destination where `maxpaths` is platform dependent.

**Default**
4

**Format**
```
maximum-paths maxpaths
```

**Mode**
Router OSPF Config
5.10.40.1 no maximum-paths
This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format: `no maximum-paths`
Mode: Router OSPF Config

5.10.41 passive-interface default (OSPF)
Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF will not form adjacencies over a passive interface.

Default: disabled
Format: `passive-interface default`
Mode: Router OSPF Config

5.10.41.1 no passive-interface default
Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to nonpassive mode.

Format: `no passive-interface default`
Mode: Router OSPF Config

5.10.42 passive-interface (OSPF)
Use this command to set the interface as passive. It overrides the global passive mode that is currently effective on the interface. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format.

Default: disabled
Format: `passive-interface {slot/port|vlan 1-4093}`
Mode: Router OSPF Config
5.10.42.1 no passive-interface

Use this command to set the interface as nonpassive. It overrides the global passive mode that is currently effective on the interface.

**Format**

no passive-interface {slot/port|vlan 1-4093}

**Mode**

Router OSPF Config

5.10.43 timers pacing flood

To adjust the rate at which OSPFv2 sends LS Update packets, use the timers pacing flood command in router OSPFv2 global configuration mode. OSPF distributes routing information in Link State Advertisements (LSAs), which are bundled into Link State Update (LS Update) packets. To reduce the likelihood of sending a neighbor more packets than it can buffer, OSPF rate limits the transmission of LS Update packets. By default, OSPF sends up to 30 updates per second on each interface (1/the pacing interval). Use this command to adjust this packet rate.

**Default**

33 milliseconds

**Format**

timers pacing flood milliseconds

**Mode**

OSPFv2 Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>milliseconds</td>
<td>The average time between transmission of LS Update packets. The range is from 5 ms to 100 ms. The default is 33 ms.</td>
</tr>
</tbody>
</table>

5.10.43.1 no timers pacing flood

To revert LSA transmit pacing to the default rate, use the no timers pacing flood command.

**Format**

no timers pacing flood

**Mode**

OSPFv2 Router Configuration

5.10.44 timers pacing lsa-group

To adjust how OSPF groups LSAs for periodic refresh, use the timers pacing lsa-group command in OSPFv2 Router Configuration mode. OSPF refreshes self-originated LSAs approximately once every 30 minutes. When OSPF refreshes LSAs, it considers all self-originated LSAs whose age is from 1800 to 1800 plus the pacing group size. Grouping LSAs for refresh allows OSPF to combine refreshed LSAs into a minimal number of LS Update packets. Minimizing the number of Update packets makes LSA distribution more efficient.

When OSPF originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPF refreshes the LSA. By selecting a random refresh delay, OSPF avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.

**Default**

60 seconds

**Format**

timers pacing lsa-group seconds

**Mode**

OSPFv2 Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Width of the window in which LSAs are refreshed. The range for the pacing group window is from 10 to 1800 seconds.</td>
</tr>
</tbody>
</table>
5.10.45 timers spf

Use this command to configure the SPF delay time and hold time. The valid range for both parameters is 0-65535 seconds.

**Default**
- delay-time—5
- hold-time—10

**Format**
```
timers spf delay-time hold-time
```

**Mode**
Router OSPF Config

5.10.46 trapflags (OSPF)

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group’s specific trapflags to enable or disable, are listed in Table 11.

<table>
<thead>
<tr>
<th>Group</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>errors</td>
<td>• authentication-failure</td>
</tr>
<tr>
<td></td>
<td>• bad-packet</td>
</tr>
<tr>
<td></td>
<td>• config-error</td>
</tr>
<tr>
<td></td>
<td>• virt-authentication-failure</td>
</tr>
<tr>
<td></td>
<td>• virt-bad-packet</td>
</tr>
<tr>
<td></td>
<td>• virt-config-error</td>
</tr>
<tr>
<td>lsa</td>
<td>• lsa-maxage</td>
</tr>
<tr>
<td></td>
<td>• lsa-originate</td>
</tr>
<tr>
<td>overflow</td>
<td>• lsdb-overflow</td>
</tr>
<tr>
<td></td>
<td>• lsdb-approaching-overflow</td>
</tr>
<tr>
<td>retransmit</td>
<td>• packets</td>
</tr>
<tr>
<td></td>
<td>• virt-packets</td>
</tr>
<tr>
<td>state-change</td>
<td>• if-state-change</td>
</tr>
<tr>
<td></td>
<td>• neighbor-state-change</td>
</tr>
<tr>
<td></td>
<td>• virtif-state-change</td>
</tr>
<tr>
<td></td>
<td>• virtneighbor-state-change</td>
</tr>
</tbody>
</table>

- To enable the individual flag, enter the group name followed by that particular flag.
- To enable all the flags in that group, give the group name followed by all.
- To enable all the flags, give the command as **trapflags all**.

**Default**
- disabled

**Format**
```
trapflags {
  all | errors {all | authentication-failure | bad-packet | config-error | virt-authentication-failure | virt-bad-packet | virt-config-error} |
  lsa {all | lsa-maxage | lsa-originate} |
  overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
  retransmit {all | packets | virt-packets} |
  state-change {all | if-state-change | neighbor-state-change | virtif-state-change | virtneighbor-state-change}
}
```

**Mode**
Router OSPF Config
5.10.46.1 no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the **group** name followed by that particular flag.
- To disable all the flags in that group, give the group name followed by **all**.
- To disable all the flags, give the command as **trapflags all**.

**Format**
```
no trapflags {
  all |
  errors {all | authentication-failure | bad-packet | config-error | virt-
            authentication-failure | virt-bad-packet | virt-config-error} |
  lsa {all | lsa-maxage | lsa-originate} |
  overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
  retransmit {all | packets | virt-packets} |
  state-change {all | if-state-change | neighbor-state-change | virtif-state-
                    change | virtneighbor-state-change}
}
```

**Mode**
- Router OSPF Config

**OSPF Interface Commands**

5.10.47 ip ospf area

Use this command to enable OSPFv2 and set the area ID of an interface or range of interfaces. The **area-id** is an IP address formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0-4294967295. This command supersedes the effects of the **network area** command. It can also be used to configure the advertiseability of the secondary addresses on this interface into the OSPFv2 domain.

**Default**
- disabled

**Format**
```
ip ospf area area-id [secondaries none]
```

**Mode**
- Interface Config

5.10.47.1 no ip ospf area

Use this command to disable OSPF on an interface.

**Format**
```
o ip ospf area [secondaries none]
```

**Mode**
- Interface Config

5.10.48 bandwidth

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the **auto-cost** command. For the purpose of the OSPF link cost calculation, use the bandwidth command to specify the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface. You can use this command to configure a single interface or a range of interfaces.

**Default**
- actual interface bandwidth

**Format**
```
bandwidth 1-10000000
```

**Mode**
- Interface Config
5.10.48.1  no bandwidth
Use this command to set the interface bandwidth to its default value.

Format  no bandwidth
Mode     Interface Config

5.10.49  ip ospf authentication
This command sets the OSPF Authentication Type and Key for the specified interface or range of interfaces. The value of type is either none, simple or encrypt. The key is composed of standard displayable, noncontrol keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. If the type is encrypt a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID. There is no default value for this command.

Format  ip ospf authentication {none | {simple key} | {encrypt key keyid}}
Mode     Interface Config

5.10.49.1  no ip ospf authentication
This command sets the default OSPF Authentication Type for the specified interface.

Format  no ip ospf authentication
Mode     Interface Config

5.10.50  ip ospf cost
This command configures the cost on an OSPF interface or range of interfaces. The cost parameter has a range of 1 to 65535.

Default  10
Format    ip ospf cost 1-65535
Mode      Interface Config
5.10.50.1  **no ip ospf cost**  
This command configures the default cost on an OSPF interface.

**Format**  
no ip ospf cost

**Mode**  
Interface Config

5.10.51  **ip ospf database-filter all out**  
Use the `ip ospf database-filter all out` command in Interface Configuration mode to disable OSPFv2 LSA flooding on an interface.

**Default**  
Disabled

**Format**  
ip ospf database-filter all out

**Mode**  
Interface Configuration

5.10.51.1  **no ip ospf database-filter all out**  
Use the `no ip ospf database-filter all out` command in Interface Configuration mode to enable OSPFv2 LSA flooding on an interface.

**Default**  
Disabled

**Format**  
no ip ospf database-filter all out

**Mode**  
Interface Configuration

5.10.52  **ip ospf dead-interval**  
This command sets the OSPF dead interval for the specified interface or range of interfaces. The value for `seconds` (range: 1–65535) is a valid positive integer, which represents the length of time in seconds that a router’s Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range in seconds from 1 to 65535.

**Default**  
40

**Format**  
ip ospf dead-interval seconds

**Mode**  
Interface Config
5.10.52.1  **no ip ospf dead-interval**

This command sets the default OSPF dead interval for the specified interface.

**Format**    no ip ospf dead-interval
**Mode**       Interface Config

5.10.53  **ip ospf hello-interval**

This command sets the OSPF hello interval for the specified interface or range of interfaces. The value for seconds is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network. Valid values range from 1 to 65535.

**Default**    10
**Format**    ip ospf hello-interval seconds
**Mode**       Interface Config

5.10.53.1  **no ip ospf hello-interval**

This command sets the default OSPF hello interval for the specified interface.

**Format**    no ip ospf hello-interval
**Mode**       Interface Config

5.10.54  **ip ospf network**

Use this command to configure OSPF to treat an interface or range of interfaces as a point-to-point rather than broadcast interface. The broadcast option sets the OSPF network type to broadcast. The point-to-point option sets the OSPF network type to point-to-point. OSPF treats interfaces as broadcast interfaces by default. (Loopback interfaces have a special loopback network type, which cannot be changed.) When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

**Default**    broadcast
**Format**    ip ospf network {broadcast | point-to-point}
**Mode**       Interface Config
5.10.54.1  no ip ospf network
Use this command to return the OSPF network type to the default.

**Format**  
no ip ospf network

**Mode**  
Interface Config

5.10.55  ip ospf prefix-suppression
This command suppresses the advertisement of the IPv4 prefixes that are associated with an interface, except for those associated with secondary IPv4 addresses. This command takes precedence over the global configuration. If this configuration is not specified, the global prefix-suppression configuration applies.

Prefix-suppression can be disabled at the interface level by using the disable option. The disable option is useful for excluding specific interfaces from performing prefix-suppression when the feature is enabled globally.

Note that the disable option disable is not equivalent to not configuring the interface specific prefix-suppression. If prefix-suppression is not configured at the interface level, the global prefix-suppression configuration is applicable for the IPv4 prefixes associated with the interface.

**Default**  
Prefix-suppression is not configured.

**Format**  
ip ospf prefix-suppression [disable]

**Mode**  
Interface Config

5.10.55.1  no ip ospf prefix-suppression
This command removes prefix-suppression configurations at the interface level. When no ip ospf prefix-suppression command is used, global prefix-suppression applies to the interface. Not configuring the command is not equal to disabling interface level prefix-suppression.

**Format**  
oip ospf prefix-suppression

**Mode**  
Interface Config

5.10.56  ip ospf priority
This command sets the OSPF priority for the specified router interface or range of interfaces. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

**Default**  
1, which is the highest router priority

**Format**  
ip ospf priority 0-255

**Mode**  
Interface Config
5.10.56.1  no ip ospf priority
This command sets the default OSPF priority for the specified router interface.

Format     no ip ospf priority
Mode       Interface Config

5.10.57    ip ospf retransmit-interval
This command sets the OSPF retransmit Interval for the specified interface or range of interfaces. The retransmit interval is specified in seconds. The value for seconds is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

Default    5
Format      ip ospf retransmit-interval 0-3600
Mode        Interface Config

5.10.57.1  no ip ospf retransmit-interval
This command sets the default OSPF retransmit Interval for the specified interface.

Format     no ip ospf retransmit-interval
Mode       Interface Config

5.10.58    ip ospf transmit-delay
This command sets the OSPF Transit Delay for the specified interface or range of interfaces. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for seconds range from 1 to 3600 (1 hour).

Default    1
Format      ip ospf transmit-delay 1-3600
Mode        Interface Config
5.10.58.1 **no ip ospf transmit-delay**

This command sets the default OSPF Transit Delay for the specified interface.

**Format**

```plaintext
no ip ospf transmit-delay
```

**Mode**

Interface Config

5.10.59 **ip ospf mtu-ignore**

This command disables OSPF maximum transmission unit (MTU) mismatch detection on an interface or range of interfaces. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

**Default**

enabled

**Format**

```plaintext
ip ospf mtu-ignore
```

**Mode**

Interface Config

5.10.59.1 **no ip ospf mtu-ignore**

This command enables the OSPF MTU mismatch detection.

**Format**

```plaintext
no ip ospf mtu-ignore
```

**Mode**

Interface Config

### IP Event Dampening Commands

5.10.60 **dampening**

Use this command to enable IP event dampening on a routing interface.

**Format**

```plaintext
dampening [half-life period] [reuse-threshold suppress-threshold max-suppress-time [restart restart-penalty]]
```

**Mode**

Interface Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Half-life period</td>
<td>The number of seconds it takes for the penalty to reduce by half. The configurable range is 1-30 seconds. Default value is 5 seconds.</td>
</tr>
<tr>
<td>Reuse Threshold</td>
<td>The value of the penalty at which the dampened interface is restored. The configurable range is 1-20,000. Default value is 1000.</td>
</tr>
<tr>
<td>Suppress Threshold</td>
<td>The value of the penalty at which the interface is dampened. The configurable range is 1-20,000. Default value is 2000.</td>
</tr>
<tr>
<td>Max Suppress Time</td>
<td>The maximum amount of time (in seconds) an interface can be in suppressed state after it stops flapping. The configurable range is 1-255 seconds. The default value is four times of half-life period. If half-period value is allowed to default, the maximum suppress time defaults to 20 seconds.</td>
</tr>
<tr>
<td>Restart Penalty</td>
<td>Penalty applied to the interface after the device reloads. The configurable range is 1-20,000. Default value is 2000.</td>
</tr>
</tbody>
</table>
5.10.60.1  no dampening
This command disables IP event dampening on a routing interface.

**Format**  
no dampening

**Mode**  
Interface Config

5.10.61  show dampening interface
This command summarizes the number of interfaces configured with dampening and the number of interfaces being suppressed.

**Format**  
show dampening interface

**Mode**  
Privileged EXEC

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

(Router)# show dampening interface
2 interfaces are configured with dampening.
1 interface is being suppressed.

5.10.62  show interface dampening
This command displays the status and configured parameters of the interfaces configured with dampening.

**Format**  
show interface dampening

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flaps</td>
<td>The number times the link state of an interface changed from UP to DOWN.</td>
</tr>
<tr>
<td>Penalty</td>
<td>Accumulated Penalty.</td>
</tr>
<tr>
<td>Supp</td>
<td>Indicates if the interface is suppressed or not.</td>
</tr>
<tr>
<td>ReuseTm</td>
<td>Number of seconds until the interface is allowed to come up again.</td>
</tr>
<tr>
<td>HalfL</td>
<td>Configured half-life period.</td>
</tr>
<tr>
<td>ReuseV</td>
<td>Configured reuse-threshold.</td>
</tr>
<tr>
<td>SuppV</td>
<td>Configured suppress threshold.</td>
</tr>
<tr>
<td>MaxSTm</td>
<td>Configured maximum suppress time in seconds.</td>
</tr>
<tr>
<td>MaxP</td>
<td>Maximum possible penalty.</td>
</tr>
<tr>
<td>Restart</td>
<td>Configured restart penalty.</td>
</tr>
</tbody>
</table>

**Note:**
1. The CLI command “clear counters” on page 155 resets the flap count to zero.
2. The interface CLI command “no shutdown” on page 292 resets the suppressed state to **False**.
3. Any change in the dampening configuration resets the current penalty, reuse time and suppressed state to their default values, meaning **0**, **0**, and **FALSE** respectively.

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

Router# show interface dampening

<table>
<thead>
<tr>
<th>Interface</th>
<th>Flaps</th>
<th>Penalty</th>
<th>Supp</th>
<th>ReuseTm</th>
<th>HalfL</th>
<th>ReuseV</th>
<th>SuppV</th>
<th>MaxSTm</th>
<th>MaxP</th>
<th>Restart</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/2</td>
<td>0</td>
<td>0</td>
<td>FALSE</td>
<td>0</td>
<td>5</td>
<td>1000</td>
<td>2000</td>
<td>20</td>
<td>16000</td>
<td>0</td>
</tr>
<tr>
<td>0/3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.10.63 OSPF Graceful Restart Commands

The OSPF protocol can be configured to participate in the checkpointing service, so that these protocols can execute a "graceful restart" when the management unit fails. In a graceful restart, the hardware to continues forwarding IPv4 packets using OSPF routes while a backup switch takes over management unit responsibility.

Graceful restart uses the concept of "helpful neighbors". A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. A planned restart is initiated by the operator through the management command `initiate failover`. The operator may initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.

5.10.64 nsf

Use this command to enable the OSPF graceful restart functionality on an interface. To disable graceful restart, use the no form of the command.

Default Disabled

Format `nsf [ietf] [planned-only]`

Modes OSPF Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ietf</td>
<td>This keyword is accepted but not required.</td>
</tr>
<tr>
<td>planned-only</td>
<td>This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).</td>
</tr>
</tbody>
</table>
5.10.64.1 no nsf
Use this command to disable graceful restart for all restarts.

5.10.65 nsf restart-interval
Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the initiate failover command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

**Default**
120 seconds

**Format**
nsf [ietf] restart-interval 1-1800

**Modes**
OSPF Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ietf</td>
<td>This keyword is accepted but not required.</td>
</tr>
<tr>
<td>seconds</td>
<td>The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.</td>
</tr>
</tbody>
</table>

5.10.65.1 no nsfrestart-interval
Use this command to revert the grace period to its default value.

**Format**
no [ietf] nsf restart-interval

**Modes**
OSPF Router Configuration

5.10.66 nsf helper
Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

**Default**
OSPF may act as a helpful neighbor for both planned and unplanned restarts

**Format**
nsf helper [planned-only]

**Modes**
OSPF Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>planned-only</td>
<td>This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.</td>
</tr>
</tbody>
</table>

5.10.66.1 no nsf helper
Use this command to disable helpful neighbor functionality for OSPF.

**Format**
no nsf helper

**Modes**
OSPF Router Configuration
5.10.67  nsf ietf helper disable
Use this command to disable helpful neighbor functionality for OSPF.

| NOTICE | The commands no nsf helper and nsf ietf helper disable are functionally equivalent. The command nsf ietf helper disable is supported solely for compatibility with other network software CLI. |

**Format**  
nsf ietf helper disable

**Modes**  
OSPF Router Configuration

5.10.68  nsf helper strict-lsa-checking
The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router. A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

**Default**  
Enabled.

**Format**  
nsf [ietf] helper strict-lsa-checking

**Modes**  
OSPF Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ietf</td>
<td>This keyword is accepted but not required.</td>
</tr>
</tbody>
</table>

5.10.68.1  no nsf [ietf] helper strict-lsa-checking
Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

**Default**  
Enabled.

**Format**  
nsf [ietf] helper strict-lsa-checking

**Modes**  
OSPF Router Configuration

OSPFv2 Stub Router Commands

5.10.69  max-metric router-lsa
To configure OSPF to enter stub router mode, use this command in Router OSPF Global Configuration mode. When OSPF is in stub router mode, as defined by RFC 3137, OSPF sets the metric in the nonstub links in its router LSA to LsInfinity. Other routers therefore compute very long paths through the stub router, and prefer any alternate path. Doing so eliminates all transit traffic through the stub router, when alternate routes are available. Stub router mode is useful when adding or removing a router from a network or to avoid transient routes when a router reloads.

You can administratively force OSPF into stub router mode. OSPF remains in stub router mode until you take OSPF out of stub router mode. Alternatively, you can configure OSPF to start in stub router mode for a configurable period of time after the router boots up.

If you set the summary LSA metric to 16,777,215, other routers will skip the summary LSA when they compute routes.

If you have configured the router to enter stub router mode on startup (max-metric router-lsa on-startup), and then enter max-metric router lsa, there is no change. If OSPF is administratively in stub router mode (the max-metric router-lsa command has been given), and you configure OSPF to enter stub router mode on startup (max-metric router-lsa on-startup), OSPF exits stub router mode (assuming the startup period has expired) and the configuration is updated.
5.10.69.1 no max-metric router-lsa

Use this command in OSPFv2 Router Configuration mode to disable stub router mode. The command clears either type of stub router mode (always or on-startup) and resets the summary-lsa option. If OSPF is configured to enter global configuration mode on startup, and during normal operation you want to immediately place OSPF in stub router mode, issue the command no max-metric router-lsa on-startup. The command no max-metric router-lsa summary-lsa causes OSPF to send summary LSAs with metrics computed using normal procedures defined in RFC 2328.

Format: no max-metric router-lsa [on-startup] [summary-lsa]
Mode: OSPFv2 Router Configuration

5.10.70 clear ip ospf stub-router

Use the clear ip ospf stub-router command in Privileged EXEC mode to force OSPF to exit stub router mode for the specified virtual router when it has automatically entered stub router mode because of a resource limitation. OSPF only exits stub router mode if it entered stub router mode because of a resource limitation or if it is in stub router mode at startup. If no virtual router is specified, the command is executed for the default router. This command has no effect if OSPF is configured to be in stub router mode permanently.

Format: clear ip ospf stub-router [vrf vrf-name]
Mode: Privileged EXEC

OSPF Show Commands

5.10.71 show ip ospf

This command displays OSPF global configuration information for the specified virtual router. If no router is specified, it displays information for the default router.

Format: show ip ospf [vrf vrf-name]
Mode: Privileged EXEC

Some of the information below displays only if you enable OSPF and configure certain features.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.</td>
</tr>
<tr>
<td>RFC 1583 Compatibility</td>
<td>Indicates whether 1583 compatibility is enabled or disabled. This is a configured value.</td>
</tr>
<tr>
<td>External LSDB Limit</td>
<td>The maximum number of nondefault AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.</td>
</tr>
<tr>
<td>Exit Overflow Interval</td>
<td>The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.</td>
</tr>
<tr>
<td>Spf Delay Time</td>
<td>The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.</td>
</tr>
<tr>
<td>Spf Hold Time</td>
<td>The number of seconds between two consecutive spf calculations.</td>
</tr>
<tr>
<td>Flood Pacing Interval</td>
<td>The average time, in milliseconds, between LS Update packet transmissions on an interface. This is the value configured with the command “timers pacing flood” on page 601.</td>
</tr>
<tr>
<td>LSA Refresh Group Pacing Time</td>
<td>The size in seconds of the LSA refresh group window. This is the value configured with the command “timers pacing lsa-group” on page 601.</td>
</tr>
<tr>
<td>Opaque Capability</td>
<td>Shows whether the router is capable of sending Opaque LSAs. This is a configured value.</td>
</tr>
<tr>
<td>Autocost Ref BW</td>
<td>Shows the value of auto-cost reference bandwidth configured on the router.</td>
</tr>
<tr>
<td>Default Passive Setting</td>
<td>Shows whether the interfaces are passive by default.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>The maximum number of paths that OSPF can report for a given destination.</td>
</tr>
<tr>
<td>Default Metric</td>
<td>Default value for redistributed routes.</td>
</tr>
<tr>
<td>Stub Router Configuration</td>
<td>When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF reoriginates its own router LSAs, setting the cost of all nonstub interfaces to infinity. Use this field to set stub router configuration to one of Always, Startup, None.</td>
</tr>
<tr>
<td>Stub Router Startup Time</td>
<td>Configured value in seconds. This row is only listed if OSPF is configured to be a stub router at startup.</td>
</tr>
<tr>
<td>Summary LSA Metric Override</td>
<td>One of Enabled (met), Disabled, where met is the metric to be sent in summary LSAs when in stub router mode.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>Indicates whether the default routes received from other source protocols are advertised or not.</td>
</tr>
<tr>
<td>Always</td>
<td>Shows whether default routes are always advertised.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric of the routes being redistributed. If the metric is not configured, this field is blank.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>Shows whether the routes are External Type 1 or External Type 2.</td>
</tr>
<tr>
<td>Number of Active Areas</td>
<td>The number of active OSPF areas. An “active” OSPF area is an area with at least one interface up.</td>
</tr>
<tr>
<td>ABR Status</td>
<td>Shows whether the router is an OSPF Area Border Router.</td>
</tr>
<tr>
<td>ASBR Status</td>
<td>Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. The router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocols. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).</td>
</tr>
<tr>
<td>Stub Router Status</td>
<td>One of Active, Inactive.</td>
</tr>
</tbody>
</table>
| Stub Router Reason | One of Configured, Startup, Resource Limitation.  
**Note:** The row is only listed if stub router is active. |
<p>| Stub Router Startup Time Remaining | The remaining time, in seconds, until OSPF exits stub router mode. This row is only listed if OSPF is in startup stub router mode. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stub Router Duration</td>
<td>The time elapsed since the router last entered the stub router mode. The row is only listed if stub router is active and the router entered stub mode because of a resource limitation. The duration is displayed in DD:HH:MM:SS format.</td>
</tr>
<tr>
<td>External LSDB Overflow</td>
<td>When the number of nondefault external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated nondefault external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.</td>
</tr>
<tr>
<td>External LSA Count</td>
<td>The number of external (LS type 5) link-state advertisements in the link-state database.</td>
</tr>
<tr>
<td>External LSA Checksum</td>
<td>The sum of the LS checksums of external link-state advertisements contained in the link-state database.</td>
</tr>
<tr>
<td>AS_OPAQUE LSA Count</td>
<td>Shows the number of ASOpaque LSAs in the link-state database.</td>
</tr>
<tr>
<td>AS_OPAQUE LSA Checksum</td>
<td>Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.</td>
</tr>
<tr>
<td>New LSAs Originated</td>
<td>The number of new link-state advertisements that have been originated.</td>
</tr>
<tr>
<td>LSAs Received</td>
<td>The number of link-state advertisements received determined to be new instantiations.</td>
</tr>
<tr>
<td>LSA Count</td>
<td>The total number of link state advertisements currently in the link state database.</td>
</tr>
<tr>
<td>Maximum Number of LSAs</td>
<td>The maximum number of LSAs that OSPF can store.</td>
</tr>
<tr>
<td>LSA High Water Mark</td>
<td>The maximum size of the link state database since the system started.</td>
</tr>
<tr>
<td>AS Scope LSA Flood List Length</td>
<td>The number of LSAs currently in the global flood queue waiting to be flooded through the OSPF domain. LSAs with AS flooding scope, such as type 5 external LSAs and type 11 Opaque LSAs.</td>
</tr>
<tr>
<td>Retransmit List Entries</td>
<td>The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.</td>
</tr>
<tr>
<td>Maximum Number of Retransmit Entries</td>
<td>The maximum number of LSAs that can be waiting for acknowledgment at any given time.</td>
</tr>
<tr>
<td>Retransmit Entries High Water Mark</td>
<td>The maximum number of LSAs on all neighbors’ retransmit lists at any given time.</td>
</tr>
<tr>
<td>NSF Support</td>
<td>Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (“Always”).</td>
</tr>
<tr>
<td>NSF Restart Interval</td>
<td>The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.</td>
</tr>
<tr>
<td>NSF Restart Status</td>
<td>The current graceful restart status of the router.</td>
</tr>
<tr>
<td></td>
<td>• Not Restarting</td>
</tr>
<tr>
<td></td>
<td>• Planned Restart</td>
</tr>
<tr>
<td></td>
<td>• Unplanned Restart</td>
</tr>
<tr>
<td>NSF Restart Age</td>
<td>Number of seconds until the graceful restart grace period expires.</td>
</tr>
<tr>
<td>NSF Restart Reason</td>
<td>Indicates why the router last exited the last restart:</td>
</tr>
<tr>
<td></td>
<td>• None — Graceful restart has not been attempted.</td>
</tr>
<tr>
<td></td>
<td>• In Progress — Restart is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Completed — The previous graceful restart completed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Timed Out — The previous graceful restart timed out.</td>
</tr>
<tr>
<td></td>
<td>• Topology Changed — The previous graceful restart terminated prematurely because of a topology change.</td>
</tr>
<tr>
<td>NSF Help Support</td>
<td>Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(alpha3) #show ip ospf

Router ID...................................... 3.3.3.3
OSPF Admin Mode................................ Enable
RFC 1583 Compatibility............................ Enable
External LDB Limit.............................. No Limit
Exit Overflow Interval......................... 0
Spf Delay Time.................................. 5
Spf Hold Time................................. 10
Flood Pacing Interval........................... 33 ms
LSA Refresh Group Pacing Time.................. 60 sec
Opaque Capability................................ Enable
AutoCost Ref BW.................................. 100 Mbps
Default Passive Setting......................... Disabled
Maximum Paths.................................. 4
Default Metric.................................... Not configured
Stub Router Configuration......................... <val>
Stub Router Startup Time......................... <val> seconds
Summary LSA Metric Override...................... Enabled (<met>)
Default Route Advertise........................ Disabled
Always............................................ FALSE
Metric........................................... Not configured
Metric Type..................................... External Type 2

Number of Active Areas......................... 1 (1 normal, 0 stub, 0 nssa)
ABR Status..................................... Disable
ASBR Status..................................... Disable
Stub Router..................................... FALSE
Stub Router Status................................ Inactive
Stub Router Reason.............................. <reason>
Stub Router Startup Time Remaining............. <duration> seconds
Stub Router Duration............................ <duration>
External LDB Overflow.......................... FALSE
External LSA Count.............................. 0
External LSA Checksum........................... 0
AS_OPAQUE LSA Count.......................... 0
AS_OPAQUE LSA Checksum........................ 0
New LSAs Originated............................. 55
LSAs Received................................... 82
LSA Count....................................... 1
Maximum Number of LSAs......................... 24200
LSA High Water Mark............................ 9
AS Scope LSA Flood List Length.................. 0
Retransmit List Entries.......................... 0
Maximum Number of Retransmit Entries......... 96800
Retransmit Entries High Water Mark............. 1
NSF Helper Support.............................. Always
NSF Helper Strict LSA Checking.................. Enabled
Prefix-suppression............................. Disabled
5.10.72  show ip ospf abr
This command displays the internal OSPF routing table entries to Area Border Routers (ABR) for the specified virtual router. If no router is specified, it displays information for the default router.

Format  
show ip ospf abr [vrf vrf-name]

Mode  
• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of the route to the destination. It can be either:</td>
</tr>
<tr>
<td></td>
<td>• intra — Intra-area route</td>
</tr>
<tr>
<td></td>
<td>• inter — Inter-area route</td>
</tr>
<tr>
<td>Router ID</td>
<td>Router ID of the destination.</td>
</tr>
<tr>
<td>Cost</td>
<td>Cost of using this route.</td>
</tr>
<tr>
<td>Area ID</td>
<td>The area ID of the area from which this route is learned.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Next hop toward the destination.</td>
</tr>
<tr>
<td>Next Hop Intf</td>
<td>The outgoing router interface to use when forwarding traffic to the next hop.</td>
</tr>
</tbody>
</table>

5.10.73  show ip ospf area
This command displays information about the area for the specified virtual router. If no router is specified, it displays information for the default router. The areaid identifies the OSPF area that is being displayed.

Format  
show ip ospf area areaid [vrf vrf-name]

Modes  
• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AreaID</td>
<td>The area id of the requested OSPF area.</td>
</tr>
<tr>
<td>External Routing</td>
<td>A number representing the external routing capabilities for this area.</td>
</tr>
<tr>
<td>Spf Runs</td>
<td>The number of times that the intra-area route table has been calculated using this area’s link-state database.</td>
</tr>
<tr>
<td>Area Border Router Count</td>
<td>The total number of area border routers reachable within this area.</td>
</tr>
<tr>
<td>Area LSA Count</td>
<td>Total number of link-state advertisements in this area’s link-state database, excluding AS External LSA’s.</td>
</tr>
<tr>
<td>Area LSA Checksum</td>
<td>A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.</td>
</tr>
<tr>
<td>Flood List Length</td>
<td>The number of LSAs waiting to be flooded within the area.</td>
</tr>
<tr>
<td>Import Summary LSAs</td>
<td>Shows whether to import summary LSAs.</td>
</tr>
<tr>
<td>OSPF Stub Metric Value</td>
<td>The metric value of the stub area. This field displays only if the area is a configured as a stub area.</td>
</tr>
</tbody>
</table>

The following OSPF NSSA specific information displays only if the area is configured as an NSSA:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Summary LSAs</td>
<td>Shows whether to import summary LSAs into the NSSA.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(R1) #show ip ospf area 1

AreaID............................... 0.0.0.1
External Routing........................ Import External LSAs
Spf Runs................................. 10
Area Border Router Count.................. 0
Area LSA Count............................ 3004
Area LSA Checksum........................ 0x5e0abed
Flood List Length........................ 0
Import Summary LSAs...................... Enable

5.10.74 show ip ospf asbr

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR) for the specified virtual router. If no router is specified, it displays information for the default router.

Format show ip ospf asbr [vrf vrf-name]

Mode
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of the route to the destination. It can be one of the following values: intra — Intra-area route inter — Inter-area route</td>
</tr>
<tr>
<td>Router ID</td>
<td>Router ID of the destination.</td>
</tr>
<tr>
<td>Cost</td>
<td>Cost of using this route.</td>
</tr>
<tr>
<td>Area ID</td>
<td>The area ID of the area from which this route is learned.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Next hop toward the destination.</td>
</tr>
<tr>
<td>Next Hop Intf</td>
<td>The outgoing router interface to use when forwarding traffic to the next hop.</td>
</tr>
</tbody>
</table>
5.10.75 show ip ospf database

This command displays information about the link state database when OSPF is enabled for the specified virtual router. If no router is specified, it displays information for the default router. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional areaid parameter to display database information about a specific area. Use the optional parameters to specify the type of link state advertisements to display.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf-name</td>
<td>Specifies the virtual router for which to display information.</td>
</tr>
<tr>
<td>asbr-summary</td>
<td>Use asbr-summary to show the autonomous system boundary router (ASBR) summary LSAs.</td>
</tr>
<tr>
<td>external</td>
<td>Use external to display the external LSAs.</td>
</tr>
<tr>
<td>network</td>
<td>Use network to display the network LSAs.</td>
</tr>
<tr>
<td>nssa-external</td>
<td>Use nssa-external to display NSSA external LSAs.</td>
</tr>
<tr>
<td>opaque-area</td>
<td>Use opaque-area to display area opaque LSAs.</td>
</tr>
<tr>
<td>opaque-as</td>
<td>Use opaque-as to display AS opaque LSAs.</td>
</tr>
<tr>
<td>opaque-link</td>
<td>Use opaque-link to display link opaque LSAs.</td>
</tr>
<tr>
<td>router</td>
<td>Use router to display router LSAs.</td>
</tr>
<tr>
<td>summary</td>
<td>Use summary to show the LSA database summary information.</td>
</tr>
<tr>
<td>lsid</td>
<td>Use lsid to specify the link state ID (LSID). The value of lsid can be an IP address or an integer in the range of 0-4294967295.</td>
</tr>
<tr>
<td>adv-router</td>
<td>Use adv-router to show the LSAs that are restricted by the advertising router.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Use self-originate to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled</td>
</tr>
</tbody>
</table>

The information below is only displayed if OSPF is enabled.

**Format**

```
```

**Mode**

- Privileged EXEC
- User EXEC

For each link-type and area, the following information is displayed:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Id</td>
<td>A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.</td>
</tr>
<tr>
<td>Adv Router</td>
<td>The Advertising Router. Is a 32-bit dotted decimal number representing the LSDB interface.</td>
</tr>
<tr>
<td>Age</td>
<td>A number representing the age of the link state advertisement in seconds.</td>
</tr>
<tr>
<td>Sequence</td>
<td>A number that represents which LSA is more recent.</td>
</tr>
<tr>
<td>Checksum</td>
<td>The total number LSA checksum.</td>
</tr>
<tr>
<td>Options</td>
<td>This is an integer. It indicates that the LSA receives special handling during routing calculations.</td>
</tr>
<tr>
<td>Rtr Opt</td>
<td>Router Options are valid for router links only.</td>
</tr>
</tbody>
</table>
5.10.76  show ip ospf database database-summary
Use this command to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database.

**Format**
```
show ip ospf database database-summary
```

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Total number of router LSAs in the OSPF link state database.</td>
</tr>
<tr>
<td>Network</td>
<td>Total number of network LSAs in the OSPF link state database.</td>
</tr>
<tr>
<td>Summary Net</td>
<td>Total number of summary network LSAs in the database.</td>
</tr>
<tr>
<td>Summary ASBR</td>
<td>Number of summary ASBR LSAs in the database.</td>
</tr>
<tr>
<td>Type-7 Ext</td>
<td>Total number of Type-7 external LSAs in the database.</td>
</tr>
<tr>
<td>Self-Originated Type-7</td>
<td>Total number of self originated AS external LSAs in the OSPF link state database.</td>
</tr>
<tr>
<td>Opaque Link</td>
<td>Number of opaque link LSAs in the database.</td>
</tr>
<tr>
<td>Opaque Area</td>
<td>Number of opaque area LSAs in the database.</td>
</tr>
<tr>
<td>Subtotal</td>
<td>Number of entries for the identified area.</td>
</tr>
<tr>
<td>Opaque AS</td>
<td>Number of opaque AS LSAs in the database.</td>
</tr>
<tr>
<td>Total</td>
<td>Number of entries for all areas.</td>
</tr>
</tbody>
</table>

5.10.77  show ip ospf interface
This command displays the information for the IFO object or virtual interface tables. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format.

**Format**
```
show ip ospf interface {slot/port|vlan 1-4093| loopback loopback-id}
```

**Mode**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address for the specified interface.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>A mask of the network and host portion of the IP address for the OSPF interface.</td>
</tr>
<tr>
<td>Secondary IP Address(es)</td>
<td>The secondary IP addresses if any are configured on the interface.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>States whether OSPF is enabled or disabled on a router interface.</td>
</tr>
<tr>
<td>OSPF Area ID</td>
<td>The OSPF Area ID for the specified interface.</td>
</tr>
<tr>
<td>OSPF Network Type</td>
<td>The type of network on this interface that the OSPF is running on.</td>
</tr>
<tr>
<td>Router Priority</td>
<td>A number representing the OSPF Priority for the specified interface.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>A number representing the OSPF Retransmit Interval for the specified interface.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>A number representing the OSPF Hello Interval for the specified interface.</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>A number representing the OSPF Dead Interval for the specified interface.</td>
</tr>
<tr>
<td>LSA Ack Interval</td>
<td>A number representing the OSPF LSA Acknowledgment Interval for the specified interface.</td>
</tr>
<tr>
<td>Transmit Delay</td>
<td>A number representing the OSPF Transmit Delay Interval for the specified interface.</td>
</tr>
</tbody>
</table>
The information below will only be displayed if OSPF is enabled.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type</td>
<td>The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.</td>
</tr>
<tr>
<td>Metric Cost</td>
<td>The cost of the OSPF interface.</td>
</tr>
<tr>
<td>Passive Status</td>
<td>Shows whether the interface is passive or not.</td>
</tr>
<tr>
<td>OSPF MTU-ignore</td>
<td>Indicates whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.</td>
</tr>
<tr>
<td>Flood Blocking</td>
<td>Indicates whether flood blocking is enabled on the interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Interface Type</td>
<td>Broadcast LANs, such as Ethernet and IEEE 802.5, take the value broadcast. The OSPF Interface Type will be ‘broadcast’.</td>
</tr>
<tr>
<td>State</td>
<td>The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>The router ID representing the designated router.</td>
</tr>
<tr>
<td>Backup Designated Router</td>
<td>The router ID representing the backup designated router.</td>
</tr>
<tr>
<td>Number of Link Events</td>
<td>The number of link events.</td>
</tr>
<tr>
<td>Local Link LSAs</td>
<td>The number of Link Local Opaque LSAs in the link-state database.</td>
</tr>
<tr>
<td>Local Link LSA Checksum</td>
<td>The sum of LS Checksums of Link Local Opaque LSAs in the link-state database.</td>
</tr>
<tr>
<td>Prefix-suppression</td>
<td>Displays whether prefix-suppression is enabled, disabled, or unconfigured on the given interface.</td>
</tr>
</tbody>
</table>

**Example:** The following shows example CLI display output for the command when the OSPF Admin Mode is disabled.

(FASTPATH Routing) > show ip ospf interface 0/1

<table>
<thead>
<tr>
<th>IP Address</th>
<th>0.0.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Secondary IP Address(es)</td>
<td></td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Disable</td>
</tr>
<tr>
<td>OSPF Area ID</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>OSPF Network Type</td>
<td>Broadcast</td>
</tr>
<tr>
<td>Router Priority</td>
<td>1</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>5</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>10</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>40</td>
</tr>
<tr>
<td>LSA Ack Interval</td>
<td>1</td>
</tr>
<tr>
<td>Transmit Delay</td>
<td>1</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>None</td>
</tr>
<tr>
<td>Metric Cost</td>
<td>1 (computed)</td>
</tr>
<tr>
<td>Passive Status</td>
<td>Non-passive interface</td>
</tr>
<tr>
<td>OSPF Mtu-ignore</td>
<td>Disable</td>
</tr>
<tr>
<td>Flood Blocking</td>
<td>Disable</td>
</tr>
</tbody>
</table>

OSPF is not enabled on this interface.

(FASTPATH Routing) #
5.10.78  show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables for the specified virtual router. If no router is specified, it displays information for the default router.

**Format**  
`show ip ospf interface brief [vrf vrf-name]`

**Mode**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>States whether OSPF is enabled or disabled on a router interface.</td>
</tr>
<tr>
<td>OSPF Area ID</td>
<td>The OSPF Area ID for the specified interface.</td>
</tr>
<tr>
<td>Router Priority</td>
<td>A number representing the OSPF Priority for the specified interface.</td>
</tr>
<tr>
<td>Cost</td>
<td>The metric cost of the OSPF interface.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>A number representing the OSPF Hello Interval for the specified interface.</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>A number representing the OSPF Dead Interval for the specified interface.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>A number representing the OSPF Retransmit Interval for the specified interface.</td>
</tr>
<tr>
<td>Interface Transmit Delay</td>
<td>A number representing the OSPF Transmit Delay for the specified interface.</td>
</tr>
<tr>
<td>LSA Ack Interval</td>
<td>A number representing the OSPF LSA Acknowledgment Interval for the specified interface.</td>
</tr>
</tbody>
</table>

5.10.79  show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format.

**Format**  
`show ip ospf interface stats {slot/port|vlan 1-4093}`

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Area ID</td>
<td>The area id of this OSPF interface.</td>
</tr>
<tr>
<td>Area Border Router Count</td>
<td>The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.</td>
</tr>
<tr>
<td>AS Border Router Count</td>
<td>The total number of Autonomous System border routers reachable within this area.</td>
</tr>
<tr>
<td>Area LSA Count</td>
<td>The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address associated with this OSPF interface.</td>
</tr>
<tr>
<td>OSPF Interface Events</td>
<td>The number of times the specified OSPF interface has changed its state, or an error has occurred.</td>
</tr>
<tr>
<td>Virtual Events</td>
<td>The number of state changes or errors that occurred on this virtual link.</td>
</tr>
<tr>
<td>Neighbor Events</td>
<td>The number of times this neighbor relationship has changed state, or an error has occurred.</td>
</tr>
<tr>
<td>Sent Packets</td>
<td>The number of OSPF packets transmitted on the interface.</td>
</tr>
<tr>
<td>Received Packets</td>
<td>The number of valid OSPF packets received on the interface.</td>
</tr>
<tr>
<td>Discards</td>
<td>The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.</td>
</tr>
</tbody>
</table>
Table 12 lists the number of OSPF packets of each type sent and received on the interface.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Version</td>
<td>The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.</td>
</tr>
<tr>
<td>Source Not On Local Subnet</td>
<td>The number of received packets discarded because the source IP address is not within a subnet configured on a local interface. Note: This field applies only to OSPFv2.</td>
</tr>
<tr>
<td>Virtual Link Not Found</td>
<td>The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet’s sender.</td>
</tr>
<tr>
<td>Area Mismatch</td>
<td>The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.</td>
</tr>
<tr>
<td>Invalid Destination Address</td>
<td>The number of OSPF packets discarded because the packet’s destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.</td>
</tr>
<tr>
<td>Wrong Authentication Type</td>
<td>The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface. Note: This field applies only to OSPFv2.</td>
</tr>
<tr>
<td>Authentication Failure</td>
<td>The number of OSPF packets dropped because the sender is not an existing neighbor or the sender’s IP address does not match the previously recorded IP address for that neighbor. Note: This field applies only to OSPFv2.</td>
</tr>
<tr>
<td>No Neighbor at Source Address</td>
<td>The number of OSPF packets dropped because the sender is not an existing neighbor or the sender’s IP address does not match the previously recorded IP address for that neighbor. Note: Does not apply to Hellos.</td>
</tr>
<tr>
<td>Invalid OSPF Packet Type</td>
<td>The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.</td>
</tr>
<tr>
<td>Hellos Ignored</td>
<td>The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.</td>
</tr>
</tbody>
</table>

Table 12: Type of OSPF Packets Sent and Received on the Interface

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>6960</td>
<td>6960</td>
</tr>
<tr>
<td>Database Description</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>LS Request</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>LS Update</td>
<td>141</td>
<td>42</td>
</tr>
<tr>
<td>LS Acknowledgment</td>
<td>40</td>
<td>135</td>
</tr>
</tbody>
</table>
5.10.80 show ip ospf lsa-group
This command displays the number of self-originated LSAs within each LSA group for the specified virtual router. If no router is specified, it displays information for the default router.

Format
show ip ospf lsa-group [vrf vrf-name]

Modes
• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total self-originated LSAs</td>
<td>The number of LSAs the router is currently originating.</td>
</tr>
<tr>
<td>Average LSAs per group</td>
<td>The number of self-originated LSAs divided by the number of LSA groups. The number of LSA groups is the refresh interval (1800 seconds) divided by the pacing interval (configured with timers pacing lsa-group) plus two.</td>
</tr>
<tr>
<td>Pacing group limit</td>
<td>The maximum number of self-originated LSAs in one LSA group. If the number of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout the refresh interval to achieve better balance.</td>
</tr>
<tr>
<td>Groups</td>
<td>For each LSA pacing group, the output shows the range of LSA ages in the group and the number of LSAs in the group.</td>
</tr>
</tbody>
</table>

5.10.81 show ip ospf neighbor
This command displays information about OSPF neighbors for the specified virtual router. If no router is specified, it displays information for the default router. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays, if the interface is a physical routing interface and vlan format if the interface is a routing vlan. The ip-address is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Format
show ip ospf neighbor [vrf vrf-name][interface {slot/port|vlan 1-4093}] [ip-address]

Modes
• Privileged EXEC
• User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The 4-digit dotted-decimal number of the neighbor router.</td>
</tr>
<tr>
<td>Priority</td>
<td>The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface of the local router in slot/port format.</td>
</tr>
</tbody>
</table>
If you specify an IP address for the neighbor router, the following fields display:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>The state of the neighboring routers. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Down—Initial state of the neighbor conversation; no recent information has been received from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Attempt—No recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Init—An Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established.</td>
</tr>
<tr>
<td></td>
<td>• 2 way—Communication between the two routers is bidirectional.</td>
</tr>
<tr>
<td></td>
<td>• Exchange start—The first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.</td>
</tr>
<tr>
<td></td>
<td>• Exchange—The router is describing its entire link state database by sending Database Description packets to the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Loading—Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.</td>
</tr>
<tr>
<td></td>
<td>• Full—The neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.</td>
</tr>
<tr>
<td><strong>Dead Time</strong></td>
<td>The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>slot/port</td>
</tr>
<tr>
<td><strong>Neighbor IP Address</strong></td>
<td>The IP address of the neighbor router.</td>
</tr>
<tr>
<td><strong>Interface Index</strong></td>
<td>The interface ID of the neighbor router.</td>
</tr>
<tr>
<td><strong>Area ID</strong></td>
<td>The area ID of the OSPF area associated with the interface.</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td>An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor’s optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.</td>
</tr>
<tr>
<td><strong>Router Priority</strong></td>
<td>The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of ‘0’ indicates that the router is not eligible to become the designated router on this network.</td>
</tr>
<tr>
<td><strong>Dead Timer Due</strong></td>
<td>The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.</td>
</tr>
<tr>
<td><strong>Up Time</strong></td>
<td>Neighbor uptime; how long since the adjacency last reached the Full state.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The state of the neighboring routers.</td>
</tr>
<tr>
<td><strong>Events</strong></td>
<td>The number of times this neighbor relationship has changed state, or an error has occurred.</td>
</tr>
<tr>
<td><strong>Retransmitted LSAs</strong></td>
<td>The number of LSAs retransmitted to this neighbor.</td>
</tr>
<tr>
<td><strong>Retransmission Queue Length</strong></td>
<td>An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.</td>
</tr>
<tr>
<td><strong>Restart Helper Status</strong></td>
<td>Indicates the status of this router as a helper during a graceful restart of the router specified in the command line:</td>
</tr>
<tr>
<td></td>
<td>• Helping—This router is acting as a helpful neighbor to this neighbor. A helpful neighbor does not report an adjacency change during graceful restart, but continues to advertise the restarting router as a FULL adjacency. A helpful neighbor continues to forward data packets to the restarting router, trusting that the restarting router’s forwarding table is maintained during the restart.</td>
</tr>
<tr>
<td></td>
<td>• Not Helping—This router is not a helpful neighbor at this time.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.
(alphal) #show ip ospf neighbor 170.1.1.50

Interface.....................................0/17
Neighbor IP Address...........................170.1.1.50
Interface Index...............................17
Area Id.......................................0.0.0.2
Options.......................................0x2
Router Priority...............................1
Dead timer due in (secs)......................15
Up Time.......................................0 days 2 hrs 8 mins 46 secs
State..........................................Full/BACKUP-DR
Events..........................................4
Retransmitted LSAs............................32
Retransmission Queue Length...............0
Restart Helper Status.........................Helping
Restart Reason...............................Software Restart (1)
Remaining Grace Time......................10 sec
Restart Helper Exit Reason..................In Progress

5.10.82 show ip ospf range

This command displays the set of OSPFv2 area ranges configured for a given area for the specified virtual router. If no router is specified, it displays information for the default router.

Format show ip ospf range areaid [vrf vrf-name]
Modes Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>The summary prefix.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnetwork mask of the summary prefix.</td>
</tr>
<tr>
<td>Type</td>
<td>S (Summary Link) or E (External Link)</td>
</tr>
</tbody>
</table>
The following shows example CLI display output for the command.

```
(R1) #show ip ospf range 0

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Subnet Mask</th>
<th>Type</th>
<th>Action</th>
<th>Cost</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.0</td>
<td>255.255.0.0</td>
<td>S</td>
<td>Advertise</td>
<td>Auto</td>
<td>N</td>
</tr>
<tr>
<td>172.20.0.0</td>
<td>255.255.0.0</td>
<td>S</td>
<td>Advertise</td>
<td>500</td>
<td>Y</td>
</tr>
</tbody>
</table>
```

### 5.10.83 show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations for the specified virtual router. If no router is specified, it displays information for the default router. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the command shows statistics for how long ago the SPF ran, how long the SPF took, the reasons why the SPF was scheduled, the individual components of the routing table calculation time and to show the RIB update time. The most recent statistics are displayed at the end of the table.

**Format**

```
show ip ospf statistics [vrf vrf-name]
```

**Modes**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delta T</td>
<td>The time since the routing table was computed. The time is in the format hours, minutes, and seconds (hh:mm:ss).</td>
</tr>
<tr>
<td>Intra</td>
<td>The time taken to compute intra-area routes, in milliseconds.</td>
</tr>
<tr>
<td>Summ</td>
<td>The time taken to compute inter-area routes, in milliseconds.</td>
</tr>
<tr>
<td>Ext</td>
<td>The time taken to compute external routes, in milliseconds.</td>
</tr>
<tr>
<td>SPF Total</td>
<td>The total time to compute routes, in milliseconds. The total may exceed the sum of the Intra, Summ, and Ext times.</td>
</tr>
<tr>
<td>RIB Update</td>
<td>The time from the completion of the routing table calculation until all changes have been made in the common routing table [the Routing Information Base (RIB)], in milliseconds.</td>
</tr>
<tr>
<td>Reason</td>
<td>The event or events that triggered the SPF. Reason codes are as follows:</td>
</tr>
<tr>
<td></td>
<td>• R - new router LSA</td>
</tr>
<tr>
<td></td>
<td>• N - new network LSA</td>
</tr>
<tr>
<td></td>
<td>• SN - new network summary LSA</td>
</tr>
<tr>
<td></td>
<td>• SA - new ASBR summary LSA</td>
</tr>
<tr>
<td></td>
<td>• X - new external LSA</td>
</tr>
</tbody>
</table>

**Example:**

The following shows example CLI display output for the command.

```
(Router) #show ip ospf statistics

Area 0.0.0.0: SPF algorithm executed 15 times

<table>
<thead>
<tr>
<th>Delta T</th>
<th>Intra</th>
<th>Summ</th>
<th>Ext</th>
<th>SPF Total</th>
<th>RIB Update</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:05:33</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R</td>
</tr>
<tr>
<td>00:05:30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R</td>
</tr>
<tr>
<td>00:05:19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>N, SN</td>
</tr>
<tr>
<td>00:05:15</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>R, N, SN</td>
</tr>
<tr>
<td>00:05:11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R</td>
</tr>
<tr>
<td>00:04:50</td>
<td>0</td>
<td>60</td>
<td>0</td>
<td>60</td>
<td>460</td>
<td>R, N</td>
</tr>
</tbody>
</table>
```
5.10.84  show ip ospf stub table

This command displays the OSPF stub table for the virtual router. If no router is specified, the information for the default router will be displayed. The information below will only be displayed if OSPF is initialized on the switch.

Format  show ip ospf stub table [vrf vrf-name]

Modes  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>A 32-bit identifier for the created stub area.</td>
</tr>
<tr>
<td>Type of Service</td>
<td>The type of service associated with the stub metric. FASTPATH only supports Normal TOS.</td>
</tr>
<tr>
<td>Metric Val</td>
<td>The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.</td>
</tr>
<tr>
<td>Import Summary LSA</td>
<td>Controls the import of summary LSAs into stub areas.</td>
</tr>
</tbody>
</table>

5.10.85  show ip ospf traffic

This command displays OSPFv2 packet and LSA statistics and OSPFv2 message queue statistics for the virtual router. If no router is specified, the information for the default router will be displayed. Packet statistics count packets and LSAs since OSPFv2 counters were last cleared (using the command “clear ip ospf counters” on page 593).

**NOTICE**
The clear ip ospf counters command does not clear the message queue high water marks.

Format  show ip ospf traffic [vrf vrf-name]

Modes  Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv2 Packet Statistics</td>
<td>The number of packets of each type sent and received since OSPF counters were last cleared.</td>
</tr>
<tr>
<td>LSAs Retransmitted</td>
<td>The number of LSAs retransmitted by this router since OSPF counters were last cleared.</td>
</tr>
<tr>
<td>LS Update Max Receive Rate</td>
<td>The maximum rate of LS Update packets received during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.</td>
</tr>
<tr>
<td>LS Update Max Send Rate</td>
<td>The maximum rate of LS Update packets transmitted during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.</td>
</tr>
<tr>
<td>Number of LSAs Received</td>
<td>The number of LSAs of each type received since OSPF counters were last cleared.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

```
(Router) #show ip ospf traffic

Time Since Counters Cleared: 4000 seconds

OSPFv2 Packet Statistics

<table>
<thead>
<tr>
<th></th>
<th>Recd:</th>
<th>Database</th>
<th>Desc</th>
<th>LS Request</th>
<th>LS Update</th>
<th>LS ACK</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent:</td>
<td>400</td>
<td>8</td>
<td>16</td>
<td>40</td>
<td>16</td>
<td>480</td>
<td></td>
</tr>
</tbody>
</table>

LSAs Retransmitted.................0
LS Update Max Receive Rate........20 pps
LS Update Max Send Rate...........10 pps

Number of LSAs Received

T1 (Router).......................10
T2 (Network)......................0
T3 (Net Summary)...............300
T4 (ASBR Summary)..............15
T5 (External).....................20
T7 (NSSA External)...............0
T9 (Link Opaque)...............0
T10 (Area Opaque)...............0
T11 (AS Opaque)...............0
Total........................345

OSPFv2 Queue Statistics

<table>
<thead>
<tr>
<th>Term</th>
<th>Current</th>
<th>Max</th>
<th>Drops</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>500</td>
</tr>
<tr>
<td>ACK</td>
<td>2</td>
<td>12</td>
<td>0</td>
<td>1600</td>
</tr>
<tr>
<td>Data</td>
<td>24</td>
<td>47</td>
<td>0</td>
<td>500</td>
</tr>
<tr>
<td>Event</td>
<td>1</td>
<td>8</td>
<td>0</td>
<td>1000</td>
</tr>
</tbody>
</table>

5.10.86  show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor for the virtual router. If no router is specified, the information for the default router will be displayed. The **areaid** parameter identifies the area and the **neighbor** parameter identifies the neighbor’s Router ID.

**Format**

```
show ip ospf virtual-link [vrf vrf-name] areaid neighbor
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>The area id of the requested OSPF area.</td>
</tr>
<tr>
<td>Neighbor Router ID</td>
<td>The input neighbor Router ID.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The configured hello interval for the OSPF virtual interface.</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>The configured dead interval for the OSPF virtual interface.</td>
</tr>
</tbody>
</table>
5.10.87 show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

**Format**
```
show ip ospf virtual-link brief
```

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>The configured transmit delay for the OSPF virtual interface.</td>
</tr>
<tr>
<td><strong>Transmit Delay</strong></td>
<td>The configured retransmit interval for the OSPF virtual interface.</td>
</tr>
<tr>
<td><strong>Retransmit Interval</strong></td>
<td>The configured authentication type of the OSPF virtual interface.</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The neighbor state.</td>
</tr>
</tbody>
</table>

5.11 Routing Information Protocol Commands

This section describes the commands you use to view and configure Routing Information Protocol (RIP), which is a distance-vector routing protocol that you use to route traffic within a small network.

5.11.1 router rip

Use this command to enter Router RIP mode.

**Format**
```
router rip
```

**Mode**
Global Config

5.11.2 enable (RIP)

This command resets the default administrative mode of RIP in the router (active).

**Default**
enabled

**Format**
enable

**Mode**
Router RIP Config
5.11.2.1 no enable (RIP)
This command sets the administrative mode of RIP in the router to inactive.

| Format   | no enable                  |
| Mode     | Router RIP Config          |

5.11.3 ip rip
This command enables RIP on a router interface or range of interfaces.

| Default  | disabled                   |
| Format   | ip rip                     |
| Mode     | Interface Config           |

5.11.3.1 no ip rip
This command disables RIP on a router interface.

| Format   | no ip rip                  |
| Mode     | Interface Config           |

5.11.4 auto-summary
This command enables the RIP auto-summarization mode.

| Default  | disabled                   |
| Format   | auto-summary               |
| Mode     | Router RIP Config          |

5.11.4.1 no auto-summary
This command disables the RIP auto-summarization mode.

| Format   | no auto-summary            |
| Mode     | Router RIP Config          |

5.11.5 default-information originate (RIP)
This command is used to control the advertisement of default routes.

| Format   | default-information originate |
| Mode     | Router RIP Config            |
5.11.5.1 no default-information originate (RIP)
This command is used to control the advertisement of default routes.

Format no default-information originate
Mode Router RIP Config

5.11.6 default-metric (RIP)
This command is used to set a default for the metric of distributed routes.

Format default-metric 0-15
Mode Router RIP Config

5.11.6.1 no default-metric (RIP)
This command is used to reset the default metric of distributed routes to its default value.

Format no default-metric
Mode Router RIP Config

5.11.7 distance rip
This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route. A route with a preference of 255 cannot be used to forward traffic.

Default 15
Format distance rip 1-255
Mode Router RIP Config

5.11.7.1 no distance rip
This command sets the default route preference value of RIP in the router.

Format no distance rip
Mode Router RIP Config

5.11.8 distribute-list out (RIP)
This command is used to specify the access list to filter routes received from the source protocol.

Default 0
Format distribute-list 1-199 out {ospf | static | connected}
Mode Router RIP Config
5.11.8.1  no distribute-list out
This command is used to specify the access list to filter routes received from the source protocol.

Format  no distribute-list 1-199 out {ospf | static | connected}
Mode    Router RIP Config

5.11.9   ip rip authentication
This command sets the RIP Version 2 Authentication Type and Key for the specified interface or range of interfaces. The value of type is either none, simple, or encrypt. The value for authentication key [key] must be 16 bytes or less. The [key] is composed of standard displayable, noncontrol keystrokes from a standard 101/102-key keyboard. If the value of type is encrypt, a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

Default  none
Format   ip rip authentication {none | {simple key} | {encrypt key keyid}}
Mode     Interface Config

5.11.9.1 no ip rip authentication
This command sets the default RIP Version 2 Authentication Type for an interface.

Format  no ip rip authentication
Mode    Interface Config

5.11.10 ip rip receive version
This command configures an interface or range of interfaces to allow RIP control packets of the specified version(s) to be received.

The value for mode is one of: rip1 to receive only RIP version 1 formatted packets, rip2 for RIP version 2, both to receive packets from either format, or none to not allow any RIP control packets to be received.

Default  both
Format   ip rip receive version {rip1 | rip2 | both | none}
Mode     Interface Config

5.11.10.1 no ip rip receive version
This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format  no ip rip receive version
Mode    Interface Config
5.11.11  ip rip send version
This command configures an interface or range of interfaces to allow RIP control packets of the specified version to be sent. The value for mode is one of: rip1 to broadcast RIP version 1 formatted packets, rip1c (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, rip2 for sending RIP version 2 using multicast, or none to not allow any RIP control packets to be sent.

Default  rip2
Format     ip rip send version {rip1 | rip1c | rip2 | none}
Mode       Interface Config

5.11.11.1 no ip rip send version
This command configures the interface to allow RIP control packets of the default version to be sent.

Format     no ip rip send version
Mode       Interface Config

5.11.12  hostroutesaccept
This command enables the RIP hostroutesaccept mode.

Default  enabled
Format hostroutesaccept
Mode       Router RIP Config

5.11.12.1 no hostroutesaccept
This command disables the RIP hostroutesaccept mode.

Format no hostroutesaccept
Mode       Router RIP Config

5.11.13  split-horizon
This command sets the RIP split horizon mode. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None - no special processing for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

Default  simple
Format split-horizon {none | simple | poison}
Mode       Router RIP Config
5.11.13.1  no split-horizon
This command sets the default RIP split horizon mode.

<table>
<thead>
<tr>
<th>Format</th>
<th>no split-horizon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Router RIP Config</td>
</tr>
</tbody>
</table>

5.11.14  redistribute (RIP)
This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match match-type the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

<table>
<thead>
<tr>
<th>Default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• metric—not-configured</td>
</tr>
<tr>
<td></td>
<td>• match—internal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Format for OSPF as source protocol</th>
<th>redistribute ospf [metric 0-15] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format for other source protocol</td>
<td>redistribute {static</td>
</tr>
<tr>
<td>Mode</td>
<td>Router RIP Config</td>
</tr>
</tbody>
</table>

5.11.14.1  no redistribute
This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

| Format       | no redistribute {ospf | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]] |
|--------------|-------------------------------------------------------------------------------------------------------------|
| Mode         | Router RIP Config                                                                                           |

5.11.15  show ip rip
This command displays information relevant to the RIP router.

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip rip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modes</td>
<td>• Privileged EXEC</td>
</tr>
<tr>
<td></td>
<td>• User EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP Admin Mode</td>
<td>Enable or disable.</td>
</tr>
<tr>
<td>Split Horizon Mode</td>
<td>None, simple or poison reverse.</td>
</tr>
<tr>
<td>Auto Summary Mode</td>
<td>Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries the default is enable.</td>
</tr>
<tr>
<td>Host Routes Accept Mode</td>
<td>Enable or disable. If enabled the router accepts host routes. The default is enable.</td>
</tr>
<tr>
<td>Global Route Changes</td>
<td>The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.</td>
</tr>
<tr>
<td>Global queries</td>
<td>The number of responses sent to RIP queries from other systems.</td>
</tr>
<tr>
<td>Default Metric</td>
<td>The default metric of redistributed routes if one has already been set, or blank if not configured earlier. The valid values are 1 to 15.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>The default route.</td>
</tr>
</tbody>
</table>
5.11.16  show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e., ip rip).

**Format**

```
show ip rip interface brief
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP source address used by the specified RIP interface.</td>
</tr>
<tr>
<td>Send Version</td>
<td>The RIP version(s) used when sending updates on the specified interface.</td>
</tr>
<tr>
<td></td>
<td>The types are none, RIP-1, RIP-1c, RIP-2.</td>
</tr>
<tr>
<td>Receive Version</td>
<td>The RIP version(s) allowed when receiving updates from the specified interface.</td>
</tr>
<tr>
<td></td>
<td>The types are none, RIP-1, RIP-2, Both.</td>
</tr>
<tr>
<td>RIP Mode</td>
<td>The administrative mode of router RIP operation (enabled or disabled).</td>
</tr>
<tr>
<td>Link State</td>
<td>The mode of the interface (up or down).</td>
</tr>
</tbody>
</table>

5.11.17  show ip rip interface

This command displays information related to a particular RIP interface. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format.

**Format**

```
show ip rip interface {slot/port|vlan 1-4093}
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td><code>slot/port</code> This is a configured value.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP source address used by the specified RIP interface. This is a configured value.</td>
</tr>
<tr>
<td>Send Version</td>
<td>The RIP version(s) used when sending updates on the specified interface.</td>
</tr>
<tr>
<td></td>
<td>The types are none, RIP-1, RIP-1c, RIP-2.</td>
</tr>
<tr>
<td>Receive Version</td>
<td>The RIP version(s) allowed when receiving updates from the specified interface.</td>
</tr>
<tr>
<td></td>
<td>The types are none, RIP-1, RIP-2, Both.</td>
</tr>
<tr>
<td>RIP Admin Mode</td>
<td>RIP administrative mode of router RIP operation; enable activates, disable de-activates it.</td>
</tr>
<tr>
<td></td>
<td>This is a configured value.</td>
</tr>
<tr>
<td>Link State</td>
<td>Indicates whether the RIP interface is up or down. This is a configured value.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.</td>
</tr>
</tbody>
</table>

The following information will be invalid if the link state is down.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Packets Received</td>
<td>The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.</td>
</tr>
<tr>
<td>Bad Routes Received</td>
<td>The number of routes contained in valid RIP packets that were ignored for any reason.</td>
</tr>
<tr>
<td>Updates Sent</td>
<td>The number of triggered RIP updates actually sent on this interface.</td>
</tr>
</tbody>
</table>
5.12  ICMP Throttling Commands
This section describes the commands you use to configure options for the transmission of various types of ICMP mes-

5.12.1   ip unreachables
Use this command to enable the generation of ICMP Destination Unreachable messages on an interface or range of inter-
faces. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default enable
Format ip unreachables
Mode Interface Config

5.12.1.1  no ip unreachables
Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format no ip unreachables
Mode Interface Config

5.12.2   ip redirects
Use this command to enable the generation of ICMP Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all inter-
faces.

Default enable
Format ip redirects
Mode • Global Config
      • Interface Config
      • Virtual Router Config

5.12.2.1  no ip redirects
Use this command to prevent the generation of ICMP Redirect messages by the router.

Format no ip redirects
Mode • Global Config
      • Interface Config

5.12.3   ipv6 redirects
Use this command to enable the generation of ICMPv6 Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all inter-
faces.

Default enable
Format ipv6 redirects
Mode Interface Config
5.12.3.1 no ipv6 redirects
Use this command to prevent the generation of ICMPv6 Redirect messages by the router.

Format: no ipv6 redirects
Mode: Interface Config

5.12.4 ip icmp echo-reply
Use this command to enable the generation of ICMP Echo Reply messages by the router. By default, the generation of ICMP Echo Reply messages is enabled.

Default: enable
Format: ip icmp echo-reply
Mode:
  • Global Config
  • Virtual Router Config

5.12.4.1 no ip icmp echo-reply
Use this command to prevent the generation of ICMP Echo Reply messages by the router.

Format: no ip icmp echo-reply
Mode: Global Config

5.12.5 ip icmp error-interval
Use this command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, burst-size and burst-interval.

The burst-interval specifies how often the token bucket is initialized with burst-size tokens. burst-interval is from 0 to 2147483647 milliseconds (msec). The burst-size is the number of ICMP error messages that can be sent during one burst-interval. The range is from 1 to 200 messages. To disable ICMP rate limiting, set burst-interval to zero (0).

Default:
  • burst-interval of 1000 msec.
  • burst-size of 100 messages

Format: ip icmp error-interval burst-interval [burst-size]
Mode:
  • Global Config
  • Virtual Router Config
5.12.5.1 no ip icmp error-interval
Use the no form of the command to return burst-interval and burst-size to their default values.

Format: no ip icmp error-interval
Mode: Global Config

5.13 Bidirectional Forwarding Detection Commands
Bidirectional Forwarding Detection (BFD) verifies bidirectional connectivity between forwarding engines, which can be a single or multi-hop away. The protocol works over any underlying transmission mechanism and protocol layer with a wide range of detection times, especially in scenarios where fast failure detection is required in data plane level for multiple concurrent sessions.

Use the following commands to configure Bidirectional Forwarding Detection commands (BFD).

5.13.1 bfd
This command enables BFD on all interfaces associated with the OSPF process.

Default: Disabled
Format: bfd
Mode: Router OSPF Config

Example: Do the following to trigger BFD processing through OSPF on all the interfaces that are associated with it.

(Router) (Config)# router ospf
(Router) (Config-router)# bfd
(Manager) (Config-router)# exit

5.13.1.1 no bfd
This command disables BFD on all interfaces associated with the OSPF process.

Format: no bfd
Mode: Router OSPF Config

5.13.2 feature bfd
This command enables BFD on the device. Note that BFD must be enabled in order to configure other protocol and interface parameters.

Default: Disabled
Format: feature bfd
Mode: Global Config
5.13.2.1 no feature bfd
Disables BFD globally and removes runtime session data. Static configurations are retained.

**Format**
```
no feature bfd
```

**Mode**
Global Config

**Example:**
```
(Router)# configure
(Router) (Config)# feature bfd
(Router) (Config)# exit
```

5.13.3 bfd echo
This command enables BFD echo mode on an IP interface.

**Default**
Disabled

**Format**
```
bfd echo
```

**Mode**
Interface Config

**Example:**
```
(Router) (Config)# interface 0/1
(Router) (Interface 0/1)# no bfd echo
(Router) (Interface 0/1)# exit
```

5.13.3.1 no bfd echo
This command disables BFD echo mode on an IP interface.

**Format**
```
no bfd echo
```

**Mode**
Interface Config

5.13.4 bfd interval
This command configures the BFD session parameters for all available interfaces on the device (Global Config mode) or IP interface (Interface Config mode). It overwrites any BFD configurations present on individual interfaces (Global Config mode) or globally configured BFD session parameters (Interface Config).

**Default**
None

**Format**
```
bfd interval transmit-interval min_rx minimum-receive-interval multiplier detection-time-multiplier
```

**Mode**
- Global Config
- Interface Config

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmit-interval</td>
<td>The desired minimum transmit interval, which is the minimum interval that the user wants to use while transmitting BFD control packets. It is represented in milliseconds. Its range is 100 ms to 1000 ms (with a change granularity of 100) with a default value of 100 ms.</td>
</tr>
<tr>
<td>minimum-receive-interval</td>
<td>The required minimum receive interval, which is the minimum interval at which the system can receive BFD control packets. It is represented in milliseconds. Its range is 100 ms to 1000 ms (with a change granularity of 100) with a default value of 100 ms.</td>
</tr>
<tr>
<td>detection-time-multiplier</td>
<td>The number of BFD control packets that must be missed in a row to declare a session down. Its range is 1 to 50 with default value of 3.</td>
</tr>
</tbody>
</table>
Example: The following steps configure BFD session parameters on the device, in Privileged EXEC mode.

```
(Router)# configure
(Router) (Config)# bfd interval 100 min_rx 200 multiplier 5
(Router) (Config)# exit
```

Example: The following steps configure BFD session parameters on an interface (for example, 0/1).

```
(Interface 0/1)# bfd interval 100 min_rx 200 multiplier 5
(Interface 0/0/1)# exit
```

5.13.4.1 no bfd interval

In Global Config mode, this command resets the BFD session parameters for all available interfaces on the device to their default values. In Interface Config mode, this command resets the BFD session parameters for all sessions on an IP interface to their default values.

Format:
```
no bfd interval
```

Mode:
- Global Config
- Interface Config

5.13.5 bfd slow-timer

This command sets up the required echo receive interval preference value. This value determines the interval the asynchronous sessions use for BFD control packets when the echo function is enabled. The slow-timer value is used as the new control packet interval, while the echo packets use the configured BFD intervals.

Default: 2000

Format:
```
bfd slow-timer echo-receive-interval
```

Mode: Global Config

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>echo-receive-interval</td>
<td>The value is represented in milliseconds. Its range is 1000 ms to 30000 ms</td>
</tr>
<tr>
<td></td>
<td>(with a change granularity of 100) with default value of 2000 ms.</td>
</tr>
</tbody>
</table>

Example:

```
(Router)# configure
(Router) (Config)# bfd slow-timer 10000
(Router) (Config)# exit
```

5.13.5.1 no bfd slow-timer

This command resets the BFD slow-timer preference value to its default.

Format: no bfd slow-timer

Mode: Global Config

5.13.6 ip ospf bfd

This command enables BFD on interfaces associated with the OSPF process.

Default: Disabled

Format: ip ospf bfd

Mode: Interface Config
5.13.6.1 no ip ospf bfd
This command disables BFD on interfaces associated with the OSPF process.

Default: Disabled
Format: no ip ospf bfd
Mode: Interface Config

5.13.7 debug bfd event
This command displays BFD state transition information.

Format: debug bfd event
Mode: Privileged EXEC

5.13.8 debug bfd packet
This command displays BFD control packet debugging information.

Format: debug bfd packet
Mode: Privileged EXEC
6 / IPv6 Management Commands

This chapter describes the IPv6 commands available in the FASTPATH CLI. This chapter contains the following sections:

- “IPv6 Management Commands” on page 644
- “Tunnel Interface Commands” on page 650
- “Loopback Interface Commands” on page 652
- “IPv6 Routing Commands” on page 652
- “OSPFv3 Commands” on page 680
- “DHCPv6 Commands” on page 714
- “DHCPv6 Snooping Configuration Commands” on page 723

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.

6.1 IPv6 Management Commands

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (i.e., independent from the IPv6 Routing package). For Routing/IPv6 builds of FASTPATH dual IPv4/IPv6 operation over the service port is enabled. FASTPATH has capabilities such as:

- Static assignment of IPv6 addresses and gateways for the service/network ports.
- The ability to ping an IPv6 link-local address over the service/network port.
- Using IPv6 Management commands, you can send SNMP traps and queries via the service/network port.
- The user can manage a device via the network port (in addition to a Routing Interface or the Service port).

6.1.1 serviceport ipv6 enable

Use this command to enable IPv6 enable on the service port. By default, IPv6 operation is enabled on the service port.

Default enabled
Format serviceport ipv6 enable
Mode Privileged EXEC
6.1.1  **no serviceport ipv6 enable**
Use this command to disable IPv6 operation on the service port.

**Format**
no serviceport ipv6 enable

**Mode**
Privileged EXEC

6.1.2  **network ipv6 enable**
Use this command to enable IPv6 operation on the network port. By default, IPv6 operation is enabled on the network port.

**Default**
enabled

**Format**
network ipv6 enable

**Mode**
Privileged EXEC

6.1.2.1  **no network ipv6 enable**
Use this command to disable IPv6 operation on the network port.

**Format**
no network ipv6 enable

**Mode**
Privileged EXEC

6.1.3  **serviceport ipv6 address**
Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information on the service port.

---

**Notice**
Multiple IPv6 prefixes can be configured on the service port.

---

**Format**

```
serviceport ipv6 address {address/prefix-length [eui64]|autoconfig|dhcp}
```

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>IPv6 prefix in IPv6 global address format.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>IPv6 prefix length value.</td>
</tr>
<tr>
<td>eui64</td>
<td>Formulate IPv6 address in eui64 address format.</td>
</tr>
<tr>
<td>autoconfig</td>
<td>Configure stateless global address autoconfiguration capability.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Configure dhcpv6 client protocol.</td>
</tr>
</tbody>
</table>
6.1.3.1 **no serviceport ipv6 address**

Use the command `no serviceport ipv6 address` to remove all configured IPv6 prefixes on the service port interface. Use the command with the address option to remove the manually configured IPv6 global address on the network port interface. Use the command with the autoconfig option to disable the stateless global address autoconfiguration on the service port. Use the command with the dhcp option to disable the dhcpv6 client protocol on the service port.

**Format**

```
no serviceport ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}
```

**Mode**

Privileged EXEC

---

### NOTICE

Only a single IPv6 gateway address can be configured for the service port. There may be a combination of IPv6 prefixes and gateways that are explicitly configured and those that are set through auto-address configuration with a connected IPv6 router on their service port interface.

**Format**

```
serviceport ipv6 gateway gateway-address
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway-address</td>
<td>Gateway address in IPv6 global or link-local address format.</td>
</tr>
</tbody>
</table>

---

#### 6.1.4 **serviceport ipv6 gateway**

Use this command to configure IPv6 gateway (i.e. Default routers) information for the service port.

**Format**

```
serviceport ipv6 gateway gateway-address
```

**Mode**

Privileged EXEC

---

#### 6.1.4.1 **no serviceport ipv6 gateway**

Use this command to remove IPv6 gateways on the service port interface.

**Format**

```
no serviceport ipv6 gateway
```

**Mode**

Privileged EXEC

---

### 6.1.5 **serviceport ipv6 neighbor**

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for the service port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

**Format**

```
serviceport ipv6 neighbor ipv6-address macaddr
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>The IPv6 address of the neighbor or interface.</td>
</tr>
<tr>
<td>macaddr</td>
<td>The link-layer address.</td>
</tr>
</tbody>
</table>
6.1.5.1  no serviceport ipv6 neighbor
Use this command to remove IPv6 neighbors from the IPv6 neighbor table for the service port.

Format  no serviceport ipv6 neighbor ipv6-address macaddr
Mode    Privileged EXEC

6.1.6  network ipv6 address
Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address autoconfiguration and to enable/disable dhcpv6 client protocol information for the network port. Multiple IPv6 addresses can be configured on the network port.

Format  network ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>IPv6 prefix in IPv6 global address format.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>IPv6 prefix length value.</td>
</tr>
<tr>
<td>eui64</td>
<td>Formulate IPv6 address in eui64 format.</td>
</tr>
<tr>
<td>autoconfig</td>
<td>Configure stateless global address autoconfiguration capability.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Configure dhcpv6 client protocol.</td>
</tr>
</tbody>
</table>

6.1.6.1  no network ipv6 address
The command no network ipv6 address removes all configured IPv6 prefixes.
Use this command with the address option to remove the manually configured IPv6 global address on the network port interface.
Use this command with the autoconfig option to disable the stateless global address autoconfiguration on the network port.
Use this command with the dhcp option disables the dhcpv6 client protocol on the network port.

Format  no network ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}
Mode    Privileged EXEC

6.1.7  network ipv6 gateway
Use this command to configure IPv6 gateway (i.e. default routers) information for the network port.

Format  network ipv6 gateway gateway-address
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway-address</td>
<td>Gateway address in IPv6 global or link-local address format.</td>
</tr>
</tbody>
</table>
6.1.7.1 no network ipv6 gateway
Use this command to remove IPv6 gateways on the network port interface.

Format  no network ipv6 gateway
Mode    Privileged EXEC

6.1.8 network ipv6 neighbor
Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for this network port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format  network ipv6 neighbor ipv6-address macaddr
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>The IPv6 address of the neighbor or interface.</td>
</tr>
<tr>
<td>macaddr</td>
<td>The link-layer address.</td>
</tr>
</tbody>
</table>

6.1.8.1 no network ipv6 neighbor
Use this command to remove IPv6 neighbors from the neighbor table.

Format  no network ipv6 neighbor ipv6-address macaddr
Mode    Privileged EXEC

6.1.9 show network ipv6 neighbors
Use this command to display the information about the IPv6 neighbor entries cached on the network port. The information is updated to show the type of the entry.

Default  None
Format   show network ipv6 neighbors
Mode     Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of the neighbor.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC Address of the neighbor.</td>
</tr>
<tr>
<td>isRtr</td>
<td>Shows if the neighbor is a router. If TRUE, the neighbor is a router; FALSE it is not a router.</td>
</tr>
<tr>
<td>Neighbor State</td>
<td>The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown</td>
</tr>
<tr>
<td>Age</td>
<td>The time in seconds that has elapsed since an entry was added to the cache.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The time in seconds that has elapsed since an entry was added to the cache.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.</td>
</tr>
</tbody>
</table>
**Example:** The following is an example of the command.

(FASTPATH Routing) #show network ipv6 neighbors

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>MAC Address</th>
<th>isRtr</th>
<th>Neighbor State</th>
<th>Age (Secs)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE80::5E26:AFF:FEBD:852C</td>
<td>5c:26:0a:bd:85:2c</td>
<td>FALSE</td>
<td>Reachable</td>
<td>0</td>
<td>Static</td>
</tr>
</tbody>
</table>

6.1.10 **show serviceport ipv6 neighbors**

Use this command to display information about the IPv6 neighbor entries cached on the service port. The information is updated to show the type of the entry.

**Default**: None

**Format**: `show serviceport ipv6 neighbors`

**Mode**: Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of the neighbor.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC Address of the neighbor.</td>
</tr>
<tr>
<td>isRtr</td>
<td>Shows if the neighbor is a router. If TRUE, the neighbor is a router; if FALSE, it is not a router.</td>
</tr>
<tr>
<td>Neighbor State</td>
<td>The state of the neighbor cache entry. The possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown.</td>
</tr>
<tr>
<td>Age</td>
<td>The time in seconds that has elapsed since an entry was added to the cache.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.</td>
</tr>
</tbody>
</table>

**Example:** The following is an example of the command.

(FASTPATH Routing) #show serviceport ipv6 neighbors

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>MAC Address</th>
<th>isRtr</th>
<th>Neighbor State</th>
<th>Age (Secs)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE80::5E26:AFF:FEBD:852C</td>
<td>5c:26:0a:bd:85:2c</td>
<td>FALSE</td>
<td>Reachable</td>
<td>0</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>

6.1.11 **ping ipv6**

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. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the `ipv6-address|hostname` parameter to ping an interface by using the global IPv6 address of the interface. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format. Use the optional `size` keyword to specify the size of the ping packet.

You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address `ipv6-global-address|hostname`. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping or traceroute request is routed out the service/network port properly. When referencing an IPv6 link-local address, you must also specify the service or network port interface by using the `serviceport` or `network` parameter.
6.1.12 ping ipv6 interface

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. You can use a loopback, network port, service port, tunnel, vlan, or physical interface as the source. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

**Format**

ping ipv6 {ipv6-global-address|hostname} / {interface {slot/port|vlan 1-4093|serviceport | network} link-local-address} [size datagram-size]

**Mode**

- Privileged EXEC
- User EXEC

---

6.2 Tunnel Interface Commands

The commands in this section describe how to create, delete, and manage tunnel interfaces. Several different types of tunnels provide functionality to facilitate the transition of IPv4 networks to IPv6 networks. These tunnels are divided into two classes: configured and automatic. The distinction is that configured tunnels are explicitly configured with a destination or endpoint of the tunnel. Automatic tunnels, in contrast, infer the endpoint of the tunnel from the destination address of packets routed into the tunnel. To assign an IP address to the tunnel interface, see "ip address" on page 515. To assign an IPv6 address to the tunnel interface, see "ipv6 address" on page 654.

### 6.2.1 interface tunnel

Use this command to enter the Interface Config mode for a tunnel interface. The tunnel-id range is 0 to 7.

**Format**

interface tunnel tunnel-id

**Mode**

Global Config
6.2.1 no interface tunnel
This command removes the tunnel interface and associated configuration parameters for the specified tunnel interface.

Format  no interface tunnel tunnel-id
Mode    Global Config

6.2.2 tunnel source
This command specifies the source transport address of the tunnel, either explicitly or by reference to an interface.

Format  tunnel source {ipv4-address | ethernet slot/port}
Mode    Interface Config

6.2.3 tunnel destination
This command specifies the destination transport address of the tunnel.

Format  tunnel destination {ipv4-address}
Mode    Interface Config

6.2.4 tunnel mode ipv6ip
This command specifies the mode of the tunnel. With the optional 6to4 argument, the tunnel mode is set to 6to4 automatic. Without the optional 6to4 argument, the tunnel mode is configured.

Format  tunnel mode ipv6ip [6to4]
Mode    Interface Config

6.2.5 show interface tunnel
This command displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

Format  show interface tunnel [tunnel-id]
Mode    Privileged EXEC

If you do not specify a tunnel ID, the command shows the following information for each configured tunnel:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel ID</td>
<td>The tunnel identification number.</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the tunnel interface.</td>
</tr>
<tr>
<td>Tunnel Mode</td>
<td>The tunnel mode.</td>
</tr>
<tr>
<td>Source Address</td>
<td>The source transport address of the tunnel.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>The destination transport address of the tunnel.</td>
</tr>
</tbody>
</table>

If you specify a tunnel ID, the command shows the following information for the tunnel:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Link Status</td>
<td>Shows whether the link is up or down.</td>
</tr>
</tbody>
</table>

www.kontron.com
# 6.3 Loopback Interface Commands

The commands in this section describe how to create, delete, and manage loopback interfaces. A loopback interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols.

To assign an IP address to the loopback interface, see "ip address" on page 515. To assign an IPv6 address to the loopback interface, see "ipv6 address" on page 654.

## 6.3.1 interface loopback

Use this command to enter the Interface Config mode for a loopback interface. The range of the loopback ID is 0 to 7.

**Format**

```
interface loopback Loopback-id
```

**Mode**

Global Config

## 6.3.1.1 no interface loopback

This command removes the loopback interface and associated configuration parameters for the specified loopback interface.

**Format**

```
no interface loopback Loopback-id
```

**Mode**

Global Config

## 6.3.2 show interface loopback

This command displays information about configured loopback interfaces.

**Format**

```
show interface loopback [Loopback-id]
```

**Mode**

Privileged EXEC

If you do not specify a loopback ID, the following information appears for each loopback interface on the system:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback ID</td>
<td>The loopback ID associated with the rest of the information in the row.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 address of the interface.</td>
</tr>
</tbody>
</table>

If you specify a loopback ID, the following information appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Link Status</td>
<td>Shows whether the link is up or down.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 address of the interface.</td>
</tr>
<tr>
<td>MTU size</td>
<td>The maximum transmission size for packets on this interface, in bytes.</td>
</tr>
</tbody>
</table>

# 6.4 IPv6 Routing Commands

This section describes the IPv6 commands you use to configure IPv6 on the system and on the interfaces. This section also describes IPv6 management commands and show commands.
6.4.1 ipv6 hop-limit
This command defines the unicast hop count used in ipv6 packets originated by the node. The value is also included in router advertisements. Valid values for hops are 1-255 inclusive. The default "not configured" means that a value of zero is sent in router advertisements and a value of 64 is sent in packets originated by the node. Note that this is not the same as configuring a value of 64.

Default: not configured
Format: ipv6 hop-limit hops
Mode: Global Config

6.4.1.1 no ipv6 hop-limit
This command returns the unicast hop count to the default.

Format: no ipv6 hop-limit
Mode: Global Config

6.4.2 ipv6 unicast-routing
Use this command to enable the forwarding of IPv6 unicast datagrams.

Default: disabled
Format: ipv6 unicast-routing
Mode: Global Config

6.4.2.1 no ipv6 unicast-routing
Use this command to disable the forwarding of IPv6 unicast datagrams.

Format: no ipv6 unicast-routing
Mode: Global Config

6.4.3 ipv6 enable
Use this command to enable IPv6 routing on an interface or range of interfaces, including tunnel and loopback interfaces, that has not been configured with an explicit IPv6 address. When you use this command, the interface is automatically configured with a link-local address. You do not need to use this command if you configured an IPv6 global address on the interface.

Default: disabled
Format: ipv6 enable
Mode: Interface Config
6.4.3.1 no ipv6 enable
Use this command to disable IPv6 routing on an interface.

**Format**
no ipv6 enable

**Mode**
Interface Config

6.4.4 ipv6 address
Use this command to configure an IPv6 address on an interface or range of interfaces, including tunnel and loopback interfaces, and to enable IPv6 processing on this interface. You can assign multiple globally reachable addresses to an interface by using this command. You do not need to assign a link-local address by using this command since one is automatically created. The `prefix` field consists of the bits of the address to be configured. The `prefix_length` designates how many of the high-order contiguous bits of the address make up the prefix.

You can express IPv6 addresses in eight blocks. Also of note is that instead of a period, a colon now separates each block. For simplification, leading zeros of each 16 bit block can be omitted. One sequence of 16 bit blocks containing only zeros can be replaced with a double colon `::`, but not more than one at a time (otherwise it is no longer a unique representation).

- Dropping zeros: `3ffe:ffff:100::f101:0:0:1` becomes `3ffe:ffff:100:f101::1`
- Local host: `0000:0000:0000:0000:0000:0000:0000:0001` becomes `::1`
- Any host: `0000:0000:0000:0000:0000:0000:0000:0000` becomes `::`

The hexadecimal letters in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is `3ffe:1::1234/64`.

The optional `[eui-64]` field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address. If you use this option, the value of `prefix_length` must be 64 bits.

**Format**
ipv6 address prefix/prefix_length [eui64]

**Mode**
Interface Config

6.4.4.1 no ipv6 address
Use this command to remove all IPv6 addresses on an interface or specified IPv6 address. The `prefix` parameter consists of the bits of the address to be configured. The `prefix_length` designates how many of the high-order contiguous bits of the address comprise the prefix. The optional `[eui-64]` field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address.

If you do not supply any parameters, the command deletes all the IPv6 addresses on an interface.

**Format**
no ipv6 address [prefix/prefix_length] [eui64]

**Mode**
Interface Config

6.4.5 ipv6 address autoconfig
Use this command to allow an in-band interface to acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages.

**Default**
disabled

**Format**
ipv6 address autoconfig

**Mode**
Interface Config
6.4.5.1 no ipv6 address autoconfig
This command the IPv6 autoconfiguration status on an interface to the default value.

Format: no ipv6 address autoconfig
Mode: Interface Config

6.4.6 ipv6 address dhcp
This command enables the DHCPv6 client on an in-band interface so that it can acquire network information, such as the IPv6 address, from a network DHCP server.

Default: disabled
Format: ipv6 address dhcp
Mode: Interface Config

6.4.6.1 no ipv6 address dhcp
This command releases a leased address and disables DHCPv6 on an interface.

Format: no ipv6 address dhcp
Mode: Interface Config

6.4.7 ipv6 route
Use this command to configure an IPv6 static route. The ipv6-prefix is the IPv6 network that is the destination of the static route. The prefix_length is the length of the IPv6 prefix — a decimal value (usually 0–64) that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the prefix_length. The next-hop-address is the IPv6 address of the next hop that can be used to reach the specified network. Specifying Null0 as nexthop parameter adds a static reject route. The preference parameter is a value the router uses to compare this route with routes from other route sources that have the same destination. The range for preference is 1–255, and the default value is 1. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format. You can specify a slot/port or vlan id or tunnel tunnel_id interface to identify direct static routes from point-to-point and broadcast interfaces. The interface must be specified when using a link-local address as the next hop. A route with a preference of 255 cannot be used to forward traffic.

Default: disabled
Format: ipv6 route ipv6-prefix/prefix_length {next-hop-address | Null0 | interface {slot/port|vlan 1-4093|tunnel tunnel_id} next-hop-address} [preference]
Mode: Global Config
6.4.7.1 no ipv6 route

Use this command to delete an IPv6 static route. Use the command without the optional parameters to delete all static routes to the specified destination. Use the `preference` parameter to revert the preference of a route to the default preference.

**Format**

no ipv6 route ipv6-prefix/prefix_length [{next-hop-address | Null0 | interface {slot/port|vlan 1-4093|tunnel tunnel_id} next-hop-address | preference}]

**Mode**

Global Config

6.4.8 ipv6 route distance

This command sets the default distance (preference) for IPv6 static routes. Lower route distance values are preferred when determining the best route. The `ipv6 route` command allows you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in this command.

Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the `ipv6 route distance` command.

**Default**

1

**Format**

ipv6 route distance 1-255

**Mode**

Global Config

6.4.8.1 no ipv6 route distance

This command resets the default static route preference value in the router to the original default preference. Lower route preference values are preferred when determining the best route.

**Format**

no ipv6 route distance

**Mode**

Global Config

6.4.9 ipv6 route net-prototype

This command adds net prototype IPv6 routes to the hardware.

**Format**

ip route net-prototype prefix/prefix-length nexthopip num-routes

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix/prefix-length</td>
<td>The destination network and mask for the route.</td>
</tr>
<tr>
<td>nexthopip</td>
<td>The next-hop ip address, it must belong to an active routing interface, but it does not need to be resolved.</td>
</tr>
<tr>
<td>num-routes</td>
<td>The number of routes need to added into hardware starting from the given prefix argument and within the given prefix-length.</td>
</tr>
</tbody>
</table>
6.4.9.1 no ipv6 route net-prototype
This command deletes all the net prototype IPv6 routes added to the hardware.

**Format**
```
ip route net-prototype prefix/prefix-length nexthopip num-routes
```

**Mode**
Global Config

6.4.10 ipv6 mtu
This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface or range of interfaces. This command replaces the default or link MTU with a new MTU value.

The default MTU value for a tunnel interface is 1480. You cannot change this value.

**Default**
0 or link speed (MTU value (1500))

**Format**
```
ipv6 mtu 1280-1500
```

**Mode**
Interface Config

6.4.10.1 no ipv6 mtu
This command resets maximum transmission unit value to default value.

**Format**
```
no ipv6 mtu
```

**Mode**
Interface Config

6.4.11 ipv6 nd dad attempts
This command sets the number of duplicate address detection probes transmitted on an interface or range of interfaces. Duplicate address detection verifies that an IPv6 address on an interface is unique.

**Default**
1

**Format**
```
ipv6 nd dad attempts 0 - 600
```

**Mode**
Interface Config
6.4.11.1  no ipv6 nd dad attempts
This command resets to number of duplicate address detection value to default value.

Format  no ipv6 nd dad attempts
Mode    Interface Config

6.4.12  ipv6 nd managed-config-flag
This command sets the "managed address configuration" flag in router advertisements on the interface or range of interfaces. When the value is true, end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

Default  false
Format    ipv6 nd managed-config-flag
Mode      Interface Config

6.4.12.1  no ipv6 nd managed-config-flag
This command resets the "managed address configuration" flag in router advertisements to the default value.

Format  no ipv6 nd managed-config-flag
Mode    Interface Config

6.4.13  ipv6 nd ns-interval
This command sets the interval between router advertisements for advertised neighbor solicitations, in milliseconds. An advertised value of 0 means the interval is unspecified. This command can configure a single interface or a range of interfaces.

Default  0
Format    ipv6 nd ns-interval \{1000-4294967295 | 0\}
Mode      Interface Config

6.4.13.1  no ipv6 nd ns-interval
This command resets the neighbor solicit retransmission interval of the specified interface to the default value.

Format  no ipv6 nd ns-interval
Mode    Interface Config

6.4.14  ipv6 nd other-config-flag
This command sets the "other stateful configuration" flag in router advertisements sent from the interface.

Default  false
Format    ipv6 nd other-config-flag
Mode      Interface Config
6.4.14.1  no ipv6 nd other-config-flag
This command resets the ‘other stateful configuration’ flag back to its default value in router advertisements sent from
the interface.

Format       no ipv6 nd other-config-flag
Mode         Interface Config

6.4.15      ipv6 nd ra-interval
This command sets the transmission interval between router advertisements on the interface or range of interfaces.

Default      600
Format        ipv6 nd ra-interval-max 4- 1800
Mode          Interface Config

6.4.15.1  no ipv6 nd ra-interval
This command sets router advertisement interval to the default.

Format       no ipv6 nd ra-interval-max
Mode          Interface Config

6.4.16      ipv6 nd ra-lifetime
This command sets the value, in seconds, that is placed in the Router Lifetime field of the router advertisements sent
from the interface or range of interfaces. The lifetime value must be zero, or it must be an integer between the value of
the router advertisement transmission interval and 9000. A value of zero means this router is not to be used as the
default router.

Default      1800
Format        ipv6 nd ra-lifetime lifetime
Mode          Interface Config

6.4.16.1  no ipv6 nd ra-lifetime
This command resets router lifetime to the default value.

Format       no ipv6 nd ra-lifetime
Mode          Interface Config

6.4.17      ipv6 nd ra hop-limit unspecified
This command configures the router to send Router Advertisements on an interface with an unspecified (0) Current Hop
Limit value. This tells the hosts on that link to ignore the Hop Limit from this Router.

Default      Disable
Format        ipv6 nd ra hop-limit unspecified
Mode          Interface Config
6.4.17.1  no ipv6 nd ra hop-limit unspecified
This command configures the router to send Router Advertisements on an interface with the global configured Hop Limit value.

Format  no ipv6 nd ra hop-limit unspecified
Mode    Interface Config

6.4.18     ipv6 nd reachable-time
This command sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation. Reachable time is specified in milliseconds. A value of zero means the time is unspecified by the router. This command can configure a single interface or a range of interfaces.

Default  0
Format    ipv6 nd reachable-time 0-4294967295
Mode      Interface Config

6.4.18.1  no ipv6 nd reachable-time
This command means reachable time is unspecified for the router.

Format    no ipv6 nd reachable-time
Mode      Interface Config

6.4.19     ipv6 nd router-preference
Use this command to configure default router preferences that the interface advertises in router advertisement messages.

Default  medium
Format    ipv6 nd router-preference { low | medium | high}
Mode      Interface Config

6.4.19.1  no ipv6 nd router-preference
This command resets the router preference advertised by the interface to the default value.

Format    no ipv6 nd router-preference
Mode      Interface Config

6.4.20     ipv6 nd suppress-ra
This command suppresses router advertisement transmission on an interface or range of interfaces.

Default  disabled
Format    ipv6 nd suppress-ra
Mode      Interface Config
6.4.20.1 no ipv6 nd suppress-ra
This command enables router transmission on an interface.

Format no ipv6 nd suppress-ra
Mode Interface Config

6.4.21 ipv6 nd prefix
Use the ipv6 nd prefix command to configure parameters associated with prefixes the router advertises in its router advertisements. The first optional parameter is the valid lifetime of the router, in seconds. You can specify a value or indicate that the lifetime value is infinite. The second optional parameter is the preferred lifetime of the router.

This command can be used to configure a single interface or a range of interfaces.

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the ipv6 address interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the ipv6 nd prefix command to configure these values.

The ipv6 nd prefix command allows you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the ipv6 address command. Prefixes specified using ipv6 nd prefix without associated interface address will not be included in RAs and will not be committed to the device configuration.

Default
- valid-lifetime—2592000
- preferred-lifetime—604800
- autoconfig—enabled
- on-link—enabled

Format ipv6 nd prefix prefix/prefix_length [{0-4294967295 | infinite} {0-4294967295 | infinite}][no-autoconfig off-link]
Mode Interface Config

6.4.21.1 no ipv6 nd prefix
This command sets prefix configuration to default values.

Format no ipv6 nd prefix prefix/prefix_length
Mode Interface Config

6.4.22 ipv6 neighbor
Configures a static IPv6 neighbor with the given IPv6 address and MAC address on a routing or host interface.

Format ipv6 neighbor ipv6address {slot/port|vlan 1-4093} macaddr
Mode Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6address</td>
<td>The IPv6 address of the neighbor.</td>
</tr>
<tr>
<td>slot/port</td>
<td>The slot/port for the interface.</td>
</tr>
<tr>
<td>vlan</td>
<td>The VLAN for the interface.</td>
</tr>
<tr>
<td>macaddr</td>
<td>The MAC address for the neighbor.</td>
</tr>
</tbody>
</table>
6.4.22.1 no ipv6 neighbor

Removes a static IPv6 neighbor with the given IPv6 address on a routing or host interface.

Format no ipv6 neighbor ipv6address {slot/port|vlan 1-4093}

6.4.23 ipv6 neighbors dynamicrenew

Use this command to automatically renew the IPv6 neighbor entries. Enables/disables the periodic NUD (neighbor unreachability detection) to be run on the existing IPv6 neighbor entries based on the activity of the entries in the hardware. If the setting is disabled, only those entries that are actively used in the hardware are triggered for NUD at the end of STALE timeout of 1200 seconds. If the setting is enabled, periodically every 40 seconds a set of 300 entries are triggered for NUD irrespective of their usage in the hardware.

Default Disabled

Format ipv6 neighbors dynamicrenew

Mode Global Config

6.4.23.1 no ipv6 neighbors dynamicrenew

Disables automatic renewing of IPv6 neighbor entries.

Format no ipv6 neighbors dynamicrenew

Mode Global Config

6.4.24 ipv6 nud

Use this command to configure Neighbor Unreachability Detection (NUD). NUD verifies that communication with a neighbor exists.

Format ipv6 nud {backoff-multiple | max-multicast-solicits | max-unicast-solicits}

Mode Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>backoff-multiple</td>
<td>Sets the exponential backoff multiple to calculate time outs in NS transmissions during NUD. The value ranges from 1 to 5. 1 is the default. The next timeout value is limited to a maximum value of 60 seconds if the value with exponential backoff calculation is greater than 60 seconds.</td>
</tr>
<tr>
<td>max-multicast-solicits</td>
<td>Sets the maximum number of multicast solicits sent during Neighbor Unreachability Detection. The value ranges from 3 to 255. 3 is the default.</td>
</tr>
<tr>
<td>max-unicast-solicits</td>
<td>Sets the maximum number of unicast solicits sent during Neighbor Unreachability Detection. The value ranges from 3 to 10. 3 is the default.</td>
</tr>
</tbody>
</table>
6.4.25  ipv6 prefix-list

To create a prefix list or add a prefix list entry, use the `ipv6 prefix-list` command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route’s prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route’s prefix using the command “match ip address” on page 539.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

**Default**

No prefix lists are configured by default. When neither the ge nor the le option is configured, the destination prefix must match the network/length exactly. If the ge option is configured without the le option, any prefix with a network mask greater than or equal to the ge value is considered a match. Similarly, if the le option is configured without the ge option, a prefix with a network mask less than or equal to the le value is considered a match.

**Format**

```
ip prefix-list list-name { [seq number] {permit | deny} ipv6-prefix/prefix-length [ge length] [le length] | renumber renumber-interval first-statement-number}
```

**Mode**

Global Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>The text name of the prefix list. Up to 32 characters.</td>
</tr>
<tr>
<td>seq number</td>
<td>(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.</td>
</tr>
<tr>
<td>permit</td>
<td>Permit routes whose destination prefix matches the statement.</td>
</tr>
<tr>
<td>deny</td>
<td>Deny routes whose destination prefix matches the statement.</td>
</tr>
<tr>
<td>ipv6-prefix/</td>
<td>Specifies the match criteria for routes being compared to the prefix list statement. The ipv6-prefix can be any valid IP prefix. The length is any IPv6 prefix length from 0 to 32.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>ge length (Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.</td>
</tr>
<tr>
<td></td>
<td>le length (Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the ge length and less than or equal to 32.</td>
</tr>
<tr>
<td>renumber</td>
<td>(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for <code>renumber-interval</code> is 1–100, and the valid range for <code>first-statement-number</code> is 1–1000.</td>
</tr>
</tbody>
</table>
6.4.25  no ip prefix-list
To delete a prefix list or a statement in a prefix list, use the no form of this command. The command no ip prefix-list list-name deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

Format  no ip prefix-list list-name [seq number] {permit | deny} network/length [ge length] [le length]
Mode    Global Configuration

6.4.26  ipv6 unreachables
Use this command to enable the generation of ICMPv6 Destination Unreachable messages on the interface or range of interfaces. By default, the generation of ICMPv6 Destination Unreachable messages is enabled.

Default  enable
Format    ipv6 unreachables
Mode      Interface Config

6.4.26.1  no ipv6 unreachables
Use this command to prevent the generation of ICMPv6 Destination Unreachable messages.

Format    no ipv6 unreachables
Mode      Interface Config

6.4.27  ipv6 unresolved-traffic
Use this command to control the rate at which IPv6 data packets come into the CPU. By default, rate limiting is disabled. When enabled, the rate can range from 50 to 1024 packets per second.

Default  enable
Format    ipv6 unresolved-traffic rate-limit <50-1024>
Mode      Global Config

6.4.27.1  no ipv6 unresolved-traffic
Use this command to disable the rate limiting.

Format    no ipv6 unresolved-traffic rate-limit
Mode      Global Config

6.4.28  ipv6 icmp error-interval
Use this command to limit the rate at which ICMPv6 error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, burst-size and burst-interval.

The burst-interval specifies how often the token bucket is initialized with burst-size tokens. burst-interval is from 0 to 2147483647 milliseconds (msec).

The burst-size is the number of ICMPv6 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages.

To disable ICMP rate limiting, set burst-interval to zero (0).
6.4.28.1 no ipv6 icmp error-interval

Use the no form of the command to return burst-interval and burst-size to their default values.

Format: no ipv6 icmp error-interval
Mode: Global Config

6.4.29 show ipv6 brief

Use this command to display the IPv6 status of forwarding mode and IPv6 unicast routing mode.

Format: show ipv6 brief
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Forwarding Mode</td>
<td>Shows whether the IPv6 forwarding mode is enabled.</td>
</tr>
<tr>
<td>IPv6 Unicast Routing Mode</td>
<td>Shows whether the IPv6 unicast routing mode is enabled.</td>
</tr>
<tr>
<td>IPv6 Hop Limit</td>
<td>Shows the unicast hop count used in IPv6 packets originated by the node. For more information, see &quot;ipv6 hop-limit&quot; on page 653.</td>
</tr>
<tr>
<td>ICMPv6 Rate Limit Error Interval</td>
<td>Shows how often the token bucket is initialized with burst-size tokens. For more information, see &quot;ipv6 icmp error-interval&quot; on page 664.</td>
</tr>
<tr>
<td>ICMPv6 Rate Limit Burst Size</td>
<td>Shows the number of ICMPv6 error messages that can be sent during one burst-interval. For more information, see &quot;ipv6 icmp error-interval&quot; on page 664.</td>
</tr>
<tr>
<td>Maximum Routes</td>
<td>Shows the maximum IPv6 route table size.</td>
</tr>
<tr>
<td>IPv6 Unresolved Data Rate Limit</td>
<td>Shows the rate in packets-per-second for the number of IPv6 data packets trapped to CPU when the packet fails to be forwarded in the hardware due to unresolved hardware address of the destined IPv6 node.</td>
</tr>
<tr>
<td>IPv6 Neighbors Dynamic Renew</td>
<td>Shows the dynamic renewal mode for the periodic NUD (neighbor unreachability detection) run on the existing IPv6 neighbor entries based on the activity of the entries in the hardware.</td>
</tr>
<tr>
<td>IPv6 NUD Maximum Unicast Solicits</td>
<td>Shows the maximum number of unicast Neighbor Solicitations sent during NUD (neighbor unreachability detection) before switching to multicast Neighbor Solicitations.</td>
</tr>
<tr>
<td>IPv6 NUD Maximum Multicast Solicits</td>
<td>Shows the maximum number of multicast Neighbor Solicitations sent during NUD (neighbor unreachability detection) when in UNREACHABLE state.</td>
</tr>
<tr>
<td>IPv6 NUD Exponential Backoff Multiple</td>
<td>Shows the exponential backoff multiple to be used in the calculation of the next timeout value for Neighbor Solicitation transmission during NUD (neighbor unreachableility detection) following the exponential backoff algorithm.</td>
</tr>
<tr>
<td>System uRPF Mode</td>
<td>Shows whether unicast Reverse Path Forwarding (uRPF) is enabled.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

```
(Switch) #show ipv6 brief

IPv6 Unicast Routing Mode...................... Disable
IPv6 Hop Limit.................................. 0
ICMPv6 Rate Limit Error Interval.............. 1000 msec
ICMPv6 Rate Limit Burst Size................... 100 messages
Maximum Routes................................. 4096
IPv6 Unresolved Data Rate Limit............... 1024 pps
IPv6 Neighbors Dynamic Renew................. Disable
IPv6 NUD Maximum Unicast Solicits............ 3
IPv6 NUD Maximum Multicast Solicits.......... 3
IPv6 NUD Exponential Backoff Multiple........ 1
System uRPF Mode............................... Enabled
```

### 6.4.30 show ipv6 interface

Use this command to show the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format. The keyword `loopback` specifies the loopback interface directly. The keyword `tunnel` specifies the IPv6 tunnel interface.

**Format**

```
show ipv6 interface {brief | slot/port|vlan 1-4093|loopback 0-7|tunnel 0-7}
```

**Mode**  Privileged EXEC

If you use the `brief` parameter, the following information displays for all configured IPv6 interfaces:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>The interface in <code>slot/port</code> format.</td>
</tr>
<tr>
<td><strong>IPv6 Operational Mode</strong></td>
<td>Shows whether the mode is enabled or disabled.</td>
</tr>
<tr>
<td><strong>IPv6 Address/Length</strong></td>
<td>Shows the IPv6 address and length on interfaces with IPv6 enabled.</td>
</tr>
<tr>
<td><strong>Method</strong></td>
<td>Indicates how each IP address was assigned. The field contains one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• DHCP - The address is leased from a DHCP server.</td>
</tr>
<tr>
<td></td>
<td>• Manual - The address is manually configured.</td>
</tr>
<tr>
<td></td>
<td>Global addresses with no annotation are assumed to be manually configured.</td>
</tr>
</tbody>
</table>

If you specify an interface, the following information also appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Routing Mode</strong></td>
<td>Shows whether IPv6 routing is enabled or disabled.</td>
</tr>
<tr>
<td><strong>IPv6 Enable Mode</strong></td>
<td>Shows whether IPv6 is enabled on the interface.</td>
</tr>
<tr>
<td><strong>Administrative Mode</strong></td>
<td>Shows whether the interface administrative mode is enabled or disabled.</td>
</tr>
<tr>
<td><strong>Bandwidth</strong></td>
<td>Shows bandwidth of the interface.</td>
</tr>
<tr>
<td><strong>Interface Maximum Transmission Unit</strong></td>
<td>The MTU size, in bytes.</td>
</tr>
<tr>
<td><strong>Router Duplicate Address Detection Transmits</strong></td>
<td>The number of consecutive duplicate address detection probes to transmit.</td>
</tr>
<tr>
<td><strong>Address Autoconfigure Mode</strong></td>
<td>Shows whether the autoconfigure mode is enabled or disabled.</td>
</tr>
<tr>
<td><strong>Address DHCP Mode</strong></td>
<td>Shows whether the DHCPv6 client is enabled on the interface.</td>
</tr>
<tr>
<td><strong>IPv6 Hop Limit Unspecified</strong></td>
<td>Indicates if the router is configured on this interface to send Router Advertisements with unspecified (0) as the Current Hop Limit value.</td>
</tr>
</tbody>
</table>
If an IPv6 prefix is configured on the interface, the following information also appears.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Prefix is</td>
<td>The IPv6 prefix for the specified interface.</td>
</tr>
<tr>
<td>Preferred Lifetime</td>
<td>The amount of time the advertised prefix is a preferred prefix.</td>
</tr>
<tr>
<td>Valid Lifetime</td>
<td>The amount of time the advertised prefix is valid.</td>
</tr>
<tr>
<td>Onlink Flag</td>
<td>Shows whether the onlink flag is set (enabled) in the prefix.</td>
</tr>
<tr>
<td>Autonomous Flag</td>
<td>Shows whether the autonomous address-configuration flag (autoconfig) is set (enabled) in the prefix.</td>
</tr>
</tbody>
</table>

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

```
(alpha-stack) #show ipv6 interface brief
```

Table:

<table>
<thead>
<tr>
<th>Oper.</th>
<th>Mode</th>
<th>IPv6 Address/Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/33</td>
<td>Enabled</td>
<td>FE80::211:88FF:FE2A:3E3C/128</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2033::211:88FF:FE2A:3E3C/64</td>
</tr>
<tr>
<td>0/17</td>
<td>Enabled</td>
<td>FE80::211:88FF:FE2A:3E3C/128</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2017::A42A:26DB:1049:43DD/128 [DHCP]</td>
</tr>
<tr>
<td>4/1</td>
<td>Enabled</td>
<td>FE80::211:88FF:FE2A:3E3C/128</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2001::211:88FF:FE2A:3E3C/64 [AUTO]</td>
</tr>
<tr>
<td>4/2</td>
<td>Disabled</td>
<td>FE80::211:88FF:FE2A:3E3C/128</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2001::211:88FF:FE2A:3E3C/64 [TENT]</td>
</tr>
</tbody>
</table>

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

```
(Switch) #show ipv6 interface 0/4/1
```

IPv6 is enabled
IPv6 Prefix is ...................... fe80::210:18ff:fe00:1105/128
2001::1/64
Routing Mode............................ Enabled
IPv6 Enable Mode.......................... Enabled
Administrative Mode........................ Enabled
IPv6 Operational Mode...................... Enabled
Bandwidth...................................... 10000 kbps
Interface Maximum Transmit Unit............ 1500

---

Router Advertisement NS Interval
The interval, in milliseconds, between router advertisements for advertised neighbor solicitations.

Router Advertisement Lifetime
Shows the router lifetime value of the interface in router advertisements.

Router Advertisement Reachable Time
The amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.

Router Advertisement Interval
The frequency, in seconds, that router advertisements are sent.

Router Advertisement Managed Config Flag
Shows whether the managed configuration flag is set (enabled) for router advertisements on this interface.

Router Advertisement Other Config Flag
Shows whether the other configuration flag is set (enabled) for router advertisements on this interface.

Router Advertisement Router Preference
Shows the router preference.

Router Advertisement Suppress Flag
Shows whether router advertisements are suppressed (enabled) or sent (disabled).

**IPv6 Destination Unreachables**
Shows whether ICMPv6 Destination Unreachable messages may be sent (enabled) or not (disabled). For more information, see “ipv6 unreachables” on page 664.

**ICMPv6 Redirect**
Specifies if ICMPv6 redirect messages are sent back to the sender by the Router in the redirect scenario is enabled on this interface.
Router Duplicate Address Detection Transmits... 1
Address DHCP Mode.......................... Disabled
IPv6 Hop Limit Unspecified............... Enabled
Router Advertisement NS Interval......... 0
Router Advertisement Lifetime.............. 1800
Router Advertisement Reachable Time.... 0
Router Advertisement Interval............. 600
Router Advertisement Managed Config Flag Disabled
Router Advertisement Other Config Flag... Disabled
Router Advertisement Router Preference... medium
Router Advertisement Suppress Flag........ Disabled
IPv6 Destination Unreachables............ Enabled
ICMPv6 Redirects......................... Enabled

Prefix 2001::1/64
Preferred Lifetime......................... 604800
Valid Lifetime............................ 2592000
Onlink Flag................................ Enabled
Autonomous Flag............................ Enabled

6.4.31  show ipv6 interface vlan

Use the show ipv6 interface vlan in Privileged EXEC mode to show the usability status of IPv6 VLAN interfaces.

Format  show ipv6 interface vlan vlan-id [prefix]
Mode    •  Privileged EXEC
         •  User EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>Valid VLAN ID</td>
</tr>
<tr>
<td>prefix</td>
<td>Display IPv6 Interface Prefix Information</td>
</tr>
</tbody>
</table>

6.4.32  show ipv6 dhcp interface

This command displays a list of all IPv6 addresses currently leased from a DHCP server on a specific in-band interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format.

Format  show ipv6 dhcp [interface {slot/port|vlan 1-4093}]
Modes   Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Displays whether the specified interface is in Client mode or not.</td>
</tr>
<tr>
<td>State</td>
<td>State of the DHCPv6 Client on this interface. The valid values are: INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND, RELEASE.</td>
</tr>
<tr>
<td>Server DUID</td>
<td>DHCPv6 Unique Identifier of the DHCPv6 Server on this interface.</td>
</tr>
<tr>
<td>T1 Time</td>
<td>The T1 time specified by the DHCPv6 server. After the client has held the address for this length of time, the client tries to renew the lease.</td>
</tr>
<tr>
<td>T2 Time</td>
<td>The T2 time specified by the DHCPv6 server. If the lease renewal fails, then when the client has held the lease for this length of time, the client sends a Rebind message to the server.</td>
</tr>
<tr>
<td>Interface IAID</td>
<td>An identifier for an identity association chosen by this client.</td>
</tr>
<tr>
<td>Leased Address</td>
<td>The IPv6 address leased by the DHCPv6 Server for this interface.</td>
</tr>
</tbody>
</table>
6.4.33 show ipv6 nd raguard policy

This command shows the status of IPv6 RA GUARD feature on the switch. It lists the ports/interfaces on which this feature is enabled and the associated device role.

**Format**

```
show ipv6 nd raguard policy
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The port/interface on which this feature is enabled.</td>
</tr>
<tr>
<td>Role</td>
<td>The associated device role for the interface.</td>
</tr>
</tbody>
</table>

**Example:**

```
(Switching) # show ipv6 nd raguard policy

Configured Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>Host</td>
</tr>
</tbody>
</table>
```

6.4.34 show ipv6 neighbors

Use this command to display information about the IPv6 neighbors.

**Format**

```
show ipv6 neighbor [interface {slot/port | vlan 1-4093 | tunnel 0-7} | ipv6-address]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface in slot/port format.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>IPv6 address of neighbor or interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Link-layer Address.</td>
</tr>
<tr>
<td>IsRtr</td>
<td>Shows whether the neighbor is a router. If the value is TRUE, the neighbor is known to be a router, and FALSE otherwise. A value of FALSE might mean that routers are not always known to be routers.</td>
</tr>
<tr>
<td>Neighbor State</td>
<td>State of neighbor cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The time in seconds that has elapsed since an entry was added to the cache.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.</td>
</tr>
</tbody>
</table>
6.4.35 clear ipv6 neighbors

Use this command to clear all entries IPv6 neighbor table or an entry on a specific interface. Use the slot/port parameter to specify the interface.

Format  clear ipv6 neighbors [slot/port]
Mode    Privileged EXEC

6.4.36 show ipv6 protocols

This command lists a summary of the configuration and status for the active IPv6 routing protocols. The command lists routing protocols that are configured and enabled. If a protocol is selected on the command line, the display is limited to that protocol.

Format  show ipv6 protocols [ospf]
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Protocol</td>
<td>OSPFv3.</td>
</tr>
<tr>
<td>Router ID</td>
<td>The router ID configured for OSPFv3.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Whether OSPF is enabled or disabled globally.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>The maximum number of next hops in an OSPF route.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>Whether OSPF is configured to originate a default route.</td>
</tr>
<tr>
<td>Always</td>
<td>Whether default advertisement depends on having a default route in the common routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric configured to be advertised with the default route.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>The metric type for the default route.</td>
</tr>
</tbody>
</table>

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

(Router) #show ipv6 protocols
Routing Protocol ......................... OSPFv3
Router ID .......................... 1.1.1.1
OSPF Admin Mode .................. Enable
Maximum Paths ......................... 4
Distance .............................. Intra 110 Inter 110 Ext 110
Default Route Advertise ............ Disabled
Always ................................ FALSE
Metric .................................. Not configured
Metric Type .......................... External Type 2
Number of Active Areas .............. 0 (0 normal, 0 stub, 0 nssa)
ABR Status .......................... Disable
ASBR Status .......................... Disable

6.4.37 show ipv6 route

This command displays the IPv6 routing table. The ipv6-address specifies a specific IPv6 address for which the best-matching route would be displayed. The ipv6-prefix/ipv6-prefix-length specifies a specific IPv6 network for which the matching route would be displayed. The interface specifies that the routes with next-hops on the interface be displayed. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format. The protocol specifies the protocol that installed the routes. The protocol is one of the following keywords: connected, ospf, static. The all specifies that all routes including best and nonbest routes are displayed. Otherwise, only the best routes are displayed.
The `show ipv6 route` command displays the routing tables in the following format:

**Codes:**
- **C** – connected,
- **S** – static
- **O** – OSPF Intra,
- **OI** – OSPF Inter,
- **OE1** – OSPF Ext 1,
- **OE2** – OSPF Ext 2
- **ON1** – OSPF NSSA Ext Type 1,
- **ON2** – OSPF NSSA Ext Type 2
- **Truncated**

The columns for the routing table display the following information:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>The code for the routing protocol that created this routing entry.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The IPv6 address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.</td>
</tr>
<tr>
<td>IPv6-Prefix/IPv6-Prefix-Length</td>
<td>The IPv6-Prefix and prefix-length of the destination IPv6 network corresponding to this route.</td>
</tr>
<tr>
<td>Preference/Metric</td>
<td>The administrative distance (preference) and cost (metric) associated with this route. An example of this output is [1/0], where 1 is the preference and 0 is the metric.</td>
</tr>
<tr>
<td>Tag</td>
<td>The decimal value of the tag associated with a redistributed route, if it is not 0.</td>
</tr>
<tr>
<td>Next-Hop</td>
<td>The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination.</td>
</tr>
<tr>
<td>Route-Timestamp</td>
<td>The last updated time for dynamic routes. The format of Route-Timestamp will be:</td>
</tr>
<tr>
<td></td>
<td>• Days:Hours:Minutes if days &gt;= 1</td>
</tr>
<tr>
<td></td>
<td>• Hours:Minutes:Seconds if days &lt; 1</td>
</tr>
<tr>
<td>Interface</td>
<td>The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be <strong>Null0</strong> interface.</td>
</tr>
<tr>
<td>T</td>
<td>A flag appended to an IPv6 route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a T after the interface name.</td>
</tr>
</tbody>
</table>

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type OSPF Inter-Area. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

**Example:** The following shows example CLI display output for the command. (FASTPATH Routing) #show ipv6 route

**IPv6 Routing Table - 3 entries**

**Codes:**
- **C** – connected,
- **S** – static
- **0** – OSPF Intra,
- **OE1** – OSPF Ext 1,
- **OE2** – OSPF Ext 2
- **ON1** – OSPF NSSA Ext Type 1,
- **ON2** – OSPF NSSA Ext Type 2
S  2001::/64 [10/0] directly connected,  Null0
C  2003::/64 [0/0]
    via ::,  0/11
S  2005::/64 [1/0]
    via 2003::2,  0/11
C  5001::/64 [0/0]
    via ::,  0/5
OE1 6001::/64 [110/1]
    via fe80::200:42ff:fe7d:2f19, 00h:00m:23s, 0/5
OI 7000::/64 [110/6]
    via fe80::200:4ff:fe35:c8bb, 00h:01m:47s, 0/11

**Example**: The following shows example CLI display output for the command to indicate a truncated route.

(router) #show ipv6 route
IPv6 Routing Table - 2 entries

Codes:  C - connected,  S - static, 6To4 - 6to4 Route  
        O - OSPF Intra,  OI - OSPF Inter,  OE1 - OSPF Ext 1, OE2 - OSPF Ext 2  
        ON1 - OSPF NSSA Ext Type 1,  ON2 - OSPF NSSA Ext Type 2

C  2001:db9:1::/64 [0/0]
    via ::,  0/1
OI 3000::/64 [110/1]
    via fe80::200:e7ff:fe2e:ec3f, 00h:00m:11s, 0/1  T

6.4.38  **show ipv6 route ecmp-groups**

This command reports all current ECMP groups in the IPv6 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv6 address and outgoing interface of each next hop in each group.

**Format**  show ipv6 route ecmp-groups

**Mode**  Privileged EXEC

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

(router) #show ipv6 route ecmp-groups

ECMP Group 1 with 2 next hops (used by 1 route)
    2001:DB8:1::1 on interface 2/1
    2001:DB8:2::14 on interface 2/2

ECMP Group 2 with 3 next hops (used by 1 route)
    2001:DB8:4::15 on interface 2/32
    2001:DB8:7::12 on interface 2/33
    2001:DB8:9::45 on interface 2/34

6.4.39  **show ipv6 route hw-failure**

Use this command to display the routes that failed to be added to the hardware due to hash errors or a table full condition.

**Format**  show ipv6 route hw-failure

**Mode**  Privileged EXEC
**Example:** The following example displays the command output.

(Routing) #show ipv6 route connected

IPv6 Routing Table - 2 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
P - Net Prototype

C 2001::/128 [0/0]
   via ::, 0/1
C 2005::/128 [0/0]
   via ::, 0/2

(Routing) #show ipv6 route hw-failure

IPv6 Routing Table - 4 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
P - Net Prototype

P 3001::/64 [0/1]
   via 2001::4, 00h:00m:04s, 0/1 hw-failure
P 3001::0:1::64 [0/1]
   via 2001::4, 00h:00m:04s, 0/1 hw-failure
P 3001::0:2::64 [0/1]
   via 2001::4, 00h:00m:04s, 0/1 hw-failure
P 3001::0:3::64 [0/1]
   via 2001::4, 00h:00m:04s, 0/1 hw-failure

6.4.40 show ipv6 route net-prototype

This command displays the net-prototype routes. The net-prototype routes are displayed with a P.

**Format**

show ipv6 route net-prototype

**Modes**

Privileged EXEC

**Example:**

(Routing) #show ipv6 route net-prototype

IPv6 Routing Table - 2 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
P - Net Prototype

P 3001::/64 [0/1]
   via 2001::4, 00h:00m:04s, 0/1
P 3001::0:1::64 [0/1]
   via 2001::4, 00h:00m:04s, 0/1

6.4.41 show ipv6 route preferences

Use this command to show the preference value associated with the type of route. Lower numbers have a greater preference. A route with a preference of 255 cannot be used to forward traffic.

**Format**

show ipv6 route preferences

**Mode**

Privileged EXEC
6.4.42 show ipv6 route summary

This command displays a summary of the state of the routing table. When the optional all keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

**Format**

```
show ipv6 route summary [all]
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Preference of directly-connected routes.</td>
</tr>
<tr>
<td>Static</td>
<td>Preference of static routes.</td>
</tr>
<tr>
<td>OSPF Intra</td>
<td>Preference of routes within the OSPF area.</td>
</tr>
<tr>
<td>OSPF Inter</td>
<td>Preference of routes to other OSPF routes that are outside of the area.</td>
</tr>
<tr>
<td>OSPF External</td>
<td>Preference of OSPF external routes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Routes</td>
<td>Total number of connected routes in the routing table.</td>
</tr>
<tr>
<td>Static Routes</td>
<td>Total number of static routes in the routing table.</td>
</tr>
<tr>
<td>OSPF Routes</td>
<td>Total number of routes installed by OSPFv3 protocol.</td>
</tr>
<tr>
<td>Reject Routes</td>
<td>Total number of reject routes installed by all protocols.</td>
</tr>
<tr>
<td>Number of Prefixes</td>
<td>Summarizes the number of routes with prefixes of different lengths.</td>
</tr>
<tr>
<td>Total Routes</td>
<td>The total number of routes in the routing table.</td>
</tr>
<tr>
<td>Best Routes</td>
<td>The number of best routes currently in the routing table. This number only</td>
</tr>
<tr>
<td></td>
<td>counts the best route to each destination.</td>
</tr>
<tr>
<td>Alternate Routes</td>
<td>The number of alternate routes currently in the routing table. An alternate</td>
</tr>
<tr>
<td></td>
<td>route is a route that was not selected as the best route to its destination.</td>
</tr>
<tr>
<td>Route Adds</td>
<td>The number of routes that have been added to the routing table.</td>
</tr>
<tr>
<td>Route Modifies</td>
<td>The number of routes that have been changed after they were initially added</td>
</tr>
<tr>
<td></td>
<td>to the routing table.</td>
</tr>
<tr>
<td>Route Deletes</td>
<td>The number of routes that have been deleted from the routing table.</td>
</tr>
<tr>
<td>Unresolved Route Adds</td>
<td>The number of route adds that failed because none of the route's next hops</td>
</tr>
<tr>
<td></td>
<td>were on a local subnet. Note that static routes can fail to be added to the</td>
</tr>
<tr>
<td></td>
<td>routing table at startup because the routing interfaces are not yet up. This</td>
</tr>
<tr>
<td></td>
<td>counter gets incremented in this case. The static routes are added to the</td>
</tr>
<tr>
<td></td>
<td>routing table when the routing interfaces come up.</td>
</tr>
<tr>
<td>Invalid Route Adds</td>
<td>The number of routes that failed to be added to the routing table because</td>
</tr>
<tr>
<td></td>
<td>the route was invalid. A log message is written for each of these failures.</td>
</tr>
<tr>
<td>Failed Route Adds</td>
<td>The number of routes that failed to be added to the routing table because</td>
</tr>
<tr>
<td></td>
<td>of a resource limitation in the routing table.</td>
</tr>
<tr>
<td>Reserved Locals</td>
<td>The number of routing table entries reserved for a local subnet on a routing</td>
</tr>
<tr>
<td></td>
<td>interface that is down. Space for local routes is always reserved so that</td>
</tr>
<tr>
<td></td>
<td>local routes can be installed when a routing interface bounces.</td>
</tr>
<tr>
<td>Unique Next Hops</td>
<td>The number of distinct next hops used among all routes currently in the rout-</td>
</tr>
<tr>
<td></td>
<td>ing table. These include local interfaces for local routes and neighbors for indirect routes.</td>
</tr>
<tr>
<td>Unique Next Hops High Water</td>
<td>The highest count of unique next hops since counters were last cleared.</td>
</tr>
<tr>
<td>Next Hop Groups</td>
<td>The current number of next hop groups in use by one or more routes. Each</td>
</tr>
<tr>
<td></td>
<td>next hop group includes one or more next hops.</td>
</tr>
<tr>
<td>Next Hop Groups High Water</td>
<td>The highest count of next hop groups since counters were last cleared.</td>
</tr>
<tr>
<td>ECMP Groups</td>
<td>The number of next hop groups with multiple next hops.</td>
</tr>
</tbody>
</table>
### Example:
The following shows example CLI display output for the command.

(FASTPATH Routing) #show ipv6 route summary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Routes</td>
<td>The number of routes with multiple next hops currently in the routing table.</td>
</tr>
<tr>
<td>Static Routes</td>
<td></td>
</tr>
<tr>
<td>6To4 Routes</td>
<td></td>
</tr>
<tr>
<td>BGP Routes</td>
<td></td>
</tr>
<tr>
<td>External Routes</td>
<td></td>
</tr>
<tr>
<td>Internal Routes</td>
<td></td>
</tr>
<tr>
<td>Local Routes</td>
<td></td>
</tr>
<tr>
<td>OSPF Routes</td>
<td></td>
</tr>
<tr>
<td>Intra Area Routes</td>
<td></td>
</tr>
<tr>
<td>Inter Area Routes</td>
<td></td>
</tr>
<tr>
<td>External Type-1 Routes</td>
<td></td>
</tr>
<tr>
<td>External Type-2 Routes</td>
<td></td>
</tr>
<tr>
<td>Reject Routes</td>
<td></td>
</tr>
<tr>
<td>Total routes</td>
<td></td>
</tr>
<tr>
<td>Best Routes (High)</td>
<td>17 (17)</td>
</tr>
<tr>
<td>Alternate Routes</td>
<td>0</td>
</tr>
<tr>
<td>Route Adds</td>
<td>44</td>
</tr>
<tr>
<td>Route Deletes</td>
<td>27</td>
</tr>
<tr>
<td>Unresolved Route Adds</td>
<td>0</td>
</tr>
<tr>
<td>Invalid Route Adds</td>
<td>0</td>
</tr>
<tr>
<td>Failed Route Adds</td>
<td>0</td>
</tr>
<tr>
<td>Reserved Locals</td>
<td>0</td>
</tr>
<tr>
<td>Unique Next Hops (High)</td>
<td>8 (8)</td>
</tr>
<tr>
<td>Next Hop Groups (High)</td>
<td>8 (8)</td>
</tr>
<tr>
<td>ECMP Groups (High)</td>
<td>3 (3)</td>
</tr>
<tr>
<td>ECMP Routes</td>
<td>12</td>
</tr>
<tr>
<td>Truncated ECMP Routes</td>
<td>0</td>
</tr>
<tr>
<td>ECMP Retries</td>
<td>0</td>
</tr>
<tr>
<td>Routes with 1 Next Hop</td>
<td>5</td>
</tr>
<tr>
<td>Routes with 2 Next Hops</td>
<td>1</td>
</tr>
<tr>
<td>Routes with 3 Next Hops</td>
<td>1</td>
</tr>
<tr>
<td>Routes with 4 Next Hops</td>
<td>10</td>
</tr>
</tbody>
</table>

Number of Prefixes:
/64: 17

### 6.4.43 show ipv6 snooping counters

This command displays the counters associated with IPv6 RA GUARD feature. The number of router advertisement and router redirect packets dropped by the switch globally due to RA GUARD feature are displayed in the command output.

**Format**

```
show ipv6 snooping counters
```

**Modes**

- Privileged EXEC
- Global Config
Example:
(Switching) # show ipv6 snooping counters

IPv6 Dropped Messages
RA(Router Advertisement - ICMP type 134)
REDIR(Router Redirect - ICMP type 137)

RA Redir
-------- --------
0 0

6.4.44 show ipv6 vlan

This command displays IPv6 VLAN routing interface addresses.

Format: show ipv6 vlan
Modes: Privileged EXEC, User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address used by Routing VLANs</td>
<td>Shows the MAC address.</td>
</tr>
</tbody>
</table>

The rest of the output for this command is displayed in a table with the following column headings:

<table>
<thead>
<tr>
<th>Column Headings</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID of a configured VLAN.</td>
</tr>
<tr>
<td>Logical Interface</td>
<td>The interface in slot/port format that is associated with the VLAN ID.</td>
</tr>
<tr>
<td>IPv6 Address/Prefix Length</td>
<td>The IPv6 prefix and prefix length associated with the VLAN ID.</td>
</tr>
</tbody>
</table>

6.4.45 show ipv6 traffic

Use this command to show traffic and statistics for IPv6 and ICMPv6. Specify a logical, loopback, or tunnel interface to view information about traffic on a specific interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format. If you do not specify an interface, the command displays information about traffic on all interfaces.

Format: show ipv6 traffic [{slot/port|vlan 1-4093| loopback loopback-id | tunnel tunnel-id}]
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Datagrams Received</td>
<td>Total number of input datagrams received by the interface, including those received in error.</td>
</tr>
<tr>
<td>Received Datagrams Locally Delivered</td>
<td>Total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter increments at the interface to which these datagrams were addressed, which might not necessarily be the input interface for some of the datagrams.</td>
</tr>
<tr>
<td>Received Datagrams Discarded Due To Header Errors</td>
<td>Number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.</td>
</tr>
<tr>
<td>Received Datagrams Discarded Due To MTU</td>
<td>Number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Received Datagrams Discarded Due To No Route</strong></td>
<td>Number of input datagrams discarded because no route could be found to transmit them to their destination.</td>
</tr>
<tr>
<td><strong>Received Datagrams With Unknown Protocol</strong></td>
<td>Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the datagrams.</td>
</tr>
<tr>
<td><strong>Received Datagrams Discarded Due To Invalid Address</strong></td>
<td>Number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0 and unsupported addresses (for example, addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.</td>
</tr>
<tr>
<td><strong>Received Datagrams Discarded Due To Truncated Data</strong></td>
<td>Number of input IPv6 datagrams for which no problems were encountered to prevent their continue processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include datagrams discarded while awaiting re-assembly.</td>
</tr>
<tr>
<td><strong>Received Datagrams Discarded Other</strong></td>
<td>Number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.</td>
</tr>
<tr>
<td><strong>Received Datagrams Reassembly Required</strong></td>
<td>Number of IPv6 datagrams successfully reassembled. Note that this counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.</td>
</tr>
<tr>
<td><strong>Datagrams Successfully Reassembled</strong></td>
<td>Number of IPv6 datagrams successfully reassembled. Note that this counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.</td>
</tr>
<tr>
<td><strong>Datagrams Failed To Reassemble</strong></td>
<td>Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in by combining them as they are received. This counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.</td>
</tr>
<tr>
<td><strong>Datagrams Forwarded</strong></td>
<td>Number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface increments.</td>
</tr>
<tr>
<td><strong>Datagrams Locally Transmitted</strong></td>
<td>Total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.</td>
</tr>
<tr>
<td><strong>Datagrams Transmit Failed</strong></td>
<td>Number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets meet this (discretionary) discard criterion.</td>
</tr>
<tr>
<td><strong>Fragments Created</strong></td>
<td>Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.</td>
</tr>
<tr>
<td><strong>Datagrams Successfully Fragmented</strong></td>
<td>Number of IPv6 datagrams that have been successfully fragmented at this output interface.</td>
</tr>
<tr>
<td><strong>Datagrams Failed To Fragment</strong></td>
<td>Number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.</td>
</tr>
<tr>
<td><strong>Fragments Created</strong></td>
<td>The number of fragments that were created.</td>
</tr>
<tr>
<td><strong>Multicast Datagrams Received</strong></td>
<td>Number of multicast packets received by the interface.</td>
</tr>
<tr>
<td><strong>Multicast Datagrams Transmitted</strong></td>
<td>Number of multicast packets transmitted by the interface.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total ICMPv6 messages received</td>
<td>Total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.</td>
</tr>
<tr>
<td>ICMPv6 Messages with errors</td>
<td>Number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).</td>
</tr>
<tr>
<td>ICMPv6 Destination Unreachable Messages Received</td>
<td>Number of ICMP Destination Unreachable messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Messages Prohibited Administratively Received</td>
<td>Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Time Exceeded Messages Received</td>
<td>Number of ICMP Time Exceeded messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Parameter Problem Messages Received</td>
<td>Number of ICMP Parameter Problem messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Packet Too Big Messages Received</td>
<td>Number of ICMP Packet Too Big messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Echo Request Messages Received</td>
<td>Number of ICMP Echo (request) messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Echo Reply Messages Received</td>
<td>Number of ICMP Echo Reply messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Router Solicit Messages Received</td>
<td>Number of ICMP Router Solicit messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Router Advertisement Messages Received</td>
<td>Number of ICMP Router Advertisement messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Neighbor Solicit Messages Received</td>
<td>Number of ICMP Neighbor Solicit messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Neighbor Advertisement Messages Received</td>
<td>Number of ICMP Neighbor Advertisement messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Redirect Messages Received</td>
<td>Number of Redirect messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Group Membership Query Messages Received</td>
<td>Number of ICMPv6 Group Membership Query messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Group Membership Response Messages Received</td>
<td>Number of ICMPv6 Group Membership response messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Group Membership Reduction Messages Received</td>
<td>Number of ICMPv6 Group Membership reduction messages received by the interface.</td>
</tr>
<tr>
<td>Total ICMPv6 Messages Transmitted</td>
<td>Total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.</td>
</tr>
<tr>
<td>ICMPv6 Messages Not Transmitted Due To Error</td>
<td>Number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter’s value.</td>
</tr>
<tr>
<td>ICMPv6 Destination Unreachable Messages Transmitted</td>
<td>Number of ICMP Destination Unreachable messages sent by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Messages Prohibited Administratively Transmitted</td>
<td>Number of ICMP destination unreachable/communication administratively prohibited messages sent.</td>
</tr>
<tr>
<td>ICMPv6 Time Exceeded Messages Transmitted</td>
<td>Number of ICMP Time Exceeded messages sent by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Parameter Problem Messages Transmitted</td>
<td>Number of ICMP Parameter Problem messages sent by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Packet Too Big Messages Transmitted</td>
<td>Number of ICMP Packet Too Big messages sent by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Echo Request Messages Transmitted</td>
<td>Number of ICMP Echo (request) messages sent by the interface.</td>
</tr>
</tbody>
</table>
6.4.46 clear ipv6 route counters

The command resets to zero the IPv6 routing table counters reported in the command "show ipv6 route summary" on page 674. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

**Format**

clear ipv6 route counters

**Mode**

Privileged EXEC

6.4.47 clear ipv6 snooping counters

This command clears the counters associated with IPv6 RA GUARD feature.

**Format**

clear ipv6 snooping counters

**Mode**

- Privileged EXEC
- Global Config

6.4.48 clear ipv6 statistics

Use this command to clear IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces. IPv6 statistics display in the output of the show ipv6 traffic command. If you do not specify an interface, the counters for all IPv6 traffic statistics reset to zero.

**Format**

clear ipv6 statistics [{slot/port | loopback Loopback-id | tunnel Tunnel-id}]

**Mode**

Privileged EXEC
6.5 OSPFv3 Commands

This section describes the commands you use to configure OSPFv3, which is a link-state routing protocol that you use to route traffic within a network. This section includes the following subsections:

- “Global OSPFv3 Commands” on page 680
- “OSPFv3 Interface Commands” on page 693
- “OSPFv3 Graceful Restart Commands” on page 697
- “OSPFv3 Stub Router Commands” on page 700
- “OSPFv3 Show Commands” on page 701

Global OSPFv3 Commands

6.5.1 ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Format: `router ospf`
Mode: Global Config

6.5.2 area default-cost (OSPFv3)

This command configures the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1–16777215.

Format: `area areaid default-cost 1-16777215`
Mode: Router OSPFv3 Config

6.5.3 area nssa (OSPFv3)

This command configures the specified areaid to function as an NSSA.

Format: `area areaid nssa`
Mode: Router OSPFv3 Config

6.5.3.1 no area nssa

This command disables nssa from the specified area id.

Format: `no area areaid nssa`
Mode: Router OSPFv3 Config

6.5.4 area nssa default-info-originate (OSPFv3)

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is 10. The metric type can be comparable (nssa-external 1) or noncomparable (nssa-external 2).

Format: `area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`
Mode: Router OSPFv3 Config
6.5.4.1 no area nssa default-info-originate (OSPFv3)
This command disables the default route advertised into the NSSA.

**Format**
```
no area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]
```

**Mode**
Router OSPFv3 Config

6.5.5 area nssa no-redistribute (OSPFv3)
This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

**Format**
```
area areaid nssa no-redistribute
```

**Mode**
Router OSPFv3 Config

6.5.5.1 no area nssa no-redistribute (OSPFv3)
This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

**Format**
```
no area areaid nssa no-redistribute
```

**Mode**
Router OSPFv3 Config

6.5.6 area nssa no-summary (OSPFv3)
This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

**Format**
```
area areaid nssa no-summary
```

**Mode**
Router OSPFv3 Config

6.5.6.1 no area nssa no-summary (OSPFv3)
This command disables nssa from the summary LSAs.

**Format**
```
no area areaid nssa no-summary
```

**Mode**
Router OSPFv3 Config

6.5.7 area nssa translator-role (OSPFv3)
This command configures the translator role of the NSSA. A value of *always* causes the router to assume the role of the translator the instant it becomes a border router and a value of *candidate* causes the router to participate in the translator election process when it attains border router status.

**Format**
```
area areaid nssa translator-role {always | candidate}
```

**Mode**
Router OSPFv3 Config
6.5.7.1 no area nssa translator-role (OSPFv3)
This command disables the nssa translator role from the specified area id.

Format: no area areaid nssa translator-role {always | candidate}
Mode: Router OSPFv3 Config

6.5.8 area nssa translator-stab-intv (OSPFv3)
This command configures the translator stability interval of the NSSA. The stability interval is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format: area areaid nssa translator-stab-intv stabilityinterval
Mode: Router OSPFv3 Config

6.5.8.1 no area nssa translator-stab-intv (OSPFv3)
This command disables the nssa translator’s stability interval from the specified area id.

Format: no area areaid nssa translator-stab-intv stabilityinterval
Mode: Router OSPFv3 Config

6.5.9 area range (OSPFv3)
Use this command to configure a summary prefix that an area border router advertises for a specific area.

Default: No area ranges are configured by default. No cost is configured by default.

Format: area area-id range prefix netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost cost]
Mode: Router OSPFv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>The area identifier for the area whose networks are to be summarized.</td>
</tr>
<tr>
<td>prefix netmask</td>
<td>The summary prefix to be advertised when the ABR computes a route to one or more networks within this prefix in this area.</td>
</tr>
<tr>
<td>summarylink</td>
<td>When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.</td>
</tr>
<tr>
<td>nssaexternallink</td>
<td>When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.</td>
</tr>
<tr>
<td>advertise</td>
<td>[Optional] When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.</td>
</tr>
<tr>
<td>not-advertise</td>
<td>[Optional] When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. When the not-advertise option is given, any static cost previously configured is removed from the system configuration.</td>
</tr>
<tr>
<td>cost</td>
<td>[Optional] If an optional cost is given, OSPF sets the metric field in the inter-area -prefix LSA to the configured value rather than setting the metric to the largest cost among the networks covered by the area range.</td>
</tr>
</tbody>
</table>
6.5.9.1 no area range
The no form of this command to delete a summary prefix or remove a static cost.

Format: no area areaid range prefix netmask {summarylink | nssaexternallink} cost
Mode: Router OSPFv3 Config

6.5.10 area stub (OSPFv3)
This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format: area areaid stub
Mode: Router OSPFv3 Config

6.5.10.1 no area stub
This command deletes a stub area for the specified area ID.

Format: no area areaid stub
Mode: Router OSPFv3 Config

6.5.11 area stub no-summary (OSPFv3)
This command disables the import of Summary LSAs for the stub area identified by areaid.

Default: enabled
Format: area areaid stub no-summary
Mode: Router OSPFv3 Config

6.5.11.1 no area stub no-summary
This command sets the Summary LSA import mode to the default for the stub area identified by areaid.

Format: no area areaid stub summarylsa
Mode: Router OSPFv3 Config

6.5.12 area virtual-link (OSPFv3)
This command creates the OSPF virtual interface for the specified areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format: area areaid virtual-link neighbor
Mode: Router OSPFv3 Config
6.5.12.1 no area virtual-link
This command deletes the OSPF virtual interface from the given interface, identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format  no area areaid virtual-link neighbor
Mode    Router OSPFv3 Config

6.5.13 area virtual-link dead-interval (OSPFv3)
This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

Default 40
Format area areaid virtual-link neighbor dead-interval seconds
Mode    Router OSPFv3 Config

6.5.13.1 no area virtual-link dead-interval
This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format  no area areaid virtual-link neighbor dead-interval
Mode    Router OSPFv3 Config

6.5.14 area virtual-link hello-interval (OSPFv3)
This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

Default 10
Format area areaid virtual-link neighbor hello-interval seconds
Mode    Router OSPFv3 Config

6.5.14.1 no area virtual-link hello-interval
This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format  no area areaid virtual-link neighbor hello-interval
Mode    Router OSPFv3 Config

6.5.15 area virtual-link retransmit-interval (OSPFv3)
This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600.

Default 5
Format area areaid virtual-link neighbor retransmit-interval seconds
Mode    Router OSPFv3 Config
6.5.15.1 no area virtual-link retransmit-interval
This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format no area areaid virtual-link neighbor retransmit-interval
Mode Router OSPFv3 Config

6.5.16 area virtual-link transmit-delay (OSPFv3)
This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600 (1 hour).

Default 1
Format area areaid virtual-link neighbor transmit-delay seconds
Mode Router OSPFv3 Config

6.5.16.1 no area virtual-link transmit-delay
This command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by areaid and neighbor. The neighbor parameter is the Router ID of the neighbor.

Format no area areaid virtual-link neighbor transmit-delay
Mode Router OSPFv3 Config

6.5.17 auto-cost (OSPFv3)
By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the auto-cost reference bandwidth and bandwidth commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where interface bandwidth is defined by the bandwidth command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the auto-cost command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1–4294967 Mbps.

Default 100Mbps
Format auto-cost reference-bandwidth 1-4294967
Mode Router OSPFv3 Config
6.5.17.1  **no auto-cost reference-bandwidth** (OSPFv3)
Use this command to set the reference bandwidth to the default value.

**Format**

no auto-cost reference-bandwidth

**Mode**

Router OSPFv3 Config

6.5.18  **clear ipv6 ospf**
Use this command to disable and re-enable OSPF.

**Format**

clear ipv6 ospf

**Mode**

Privileged EXEC

6.5.19  **clear ipv6 ospf configuration**
Use this command to reset the OSPF configuration to factory defaults.

**Format**

clear ipv6 ospf configuration

**Mode**

Privileged EXEC

6.5.20  **clear ipv6 ospf counters**
Use this command to reset global and interface statistics.

**Format**

clear ipv6 ospf counters

**Mode**

Privileged EXEC

6.5.21  **clear ipv6 ospf neighbor**
Use this command to drop the adjacency with all OSPF neighbors. On each neighbor’s interface, send a one-way hello. Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor’s Router ID using the optional parameter `neighbor-id`.

**Format**

clear ipv6 ospf neighbor [neighbor-id]

**Mode**

Privileged EXEC

6.5.22  **clear ipv6 ospf neighbor interface**
To drop adjacency with all neighbors on a specific interface, use the optional parameter `[slot/port]`. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format. To drop adjacency with a specific router ID on a specific interface, use the optional parameter `neighbor-id`.

**Format**

clear ipv6 ospf neighbor interface [slot/port|vlan 1-4093] [neighbor-id]

**Mode**

Privileged EXEC
6.5.23 clear ipv6 ospf redistribution
Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

Format   clear ipv6 ospf redistribution
Mode     Privileged EXEC

6.5.24 default-information originate (OSPFv3)
This command is used to control the advertisement of default routes.

Default  • metric—unspecified
         • type—2
Format    default-information originate [always] [metric 0-16777214] [metric-type {1 | 2}]
Mode      Router OSPFv3 Config

6.5.24.1 no default-information originate (OSPFv3)
This command is used to control the advertisement of default routes.

Format    no default-information originate [metric] [metric-type]
Mode      Router OSPFv3 Config

6.5.25 default-metric (OSPFv3)
This command is used to set a default for the metric of distributed routes.

Format    default-metric 1-16777214
Mode      Router OSPFv3 Config

6.5.25.1 no default-metric (OSPFv3)
This command is used to set a default for the metric of distributed routes.

Format    no default-metric
Mode      Router OSPFv3 Config

6.5.26 distance ospf (OSPFv3)
This command sets the route preference value of OSPF route types in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value. The range of preference value is 1 to 255.

Default  110
Format    distance ospf {intra-area 1-255 | inter-area 1-255 | external 1-255}
Mode      Router OSPFv3 Config
6.5.26.1 no distance ospf
This command sets the default route preference value of OSPF routes in the router. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value.

**Format**

```
no distance ospf {intra-area | inter-area | external}
```

**Mode**

Router OSPFv3 Config

6.5.27 enable (OSPFv3)
This command resets the default administrative mode of OSPF in the router (active).

**Default**

enabled

**Format**

```
enable
```

**Mode**

Router OSPFv3 Config

6.5.27.1 no enable (OSPFv3)
This command sets the administrative mode of OSPF in the router to inactive.

**Format**

```
no enable
```

**Mode**

Router OSPFv3 Config

6.5.28 exit-overflow-interval (OSPFv3)
This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave overflow state until restarted. The range for **seconds** is 0 to 2147483647 seconds.

**Default**

0

**Format**

```
exit-overflow-interval seconds
```

**Mode**

Router OSPFv3 Config

6.5.28.1 no exit-overflow-interval
This command configures the default exit overflow interval for OSPF.

**Format**

```
no exit-overflow-interval
```

**Mode**

Router OSPFv3 Config

6.5.29 external-lsdb-limit (OSPFv3)
This command configures the external LSDB limit for OSPF. If the value is –1, then there is no limit. When the number of nondefault AS-external-LSAs in a router’s link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit nondefault AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for **limit** is –1 to 2147483647.

**Default**

-1

**Format**

```
external-lsdb-limit limit
```

**Mode**

Router OSPFv3 Config
6.5.29.1 no external-lsdb-limit
This command configures the default external LSDB limit for OSPF.

Format no external-lsdb-limit
Mode Router OSPFv3 Config

6.5.30 maximum-paths (OSPFv3)
This command sets the number of paths that OSPF can report for a given destination where maxpaths is platform dependent.

Default 4
Format maximum-paths maxpaths
Mode Router OSPFv3 Config

6.5.30.1 no maximum-paths
This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format no maximum-paths
Mode Router OSPFv3 Config

6.5.31 passive-interface default (OSPFv3)
Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF shall not form adjacencies over a passive interface.

Default disabled
Format passive-interface default
Mode Router OSPFv3 Config

6.5.31.1 no passive-interface default
Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to nonpassive mode.

Format no passive-interface default
Mode Router OSPFv3 Config

6.5.32 passive-interface (OSPFv3)
Use this command to set the interface or tunnel as passive. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format. It overrides the global passive mode that is currently effective on the interface or tunnel.

Default disabled
Format passive-interface {slot/port|vlan 1-4093|tunnel tunnel-id}
Mode Router OSPFv3 Config
6.5.32.1 no passive-interface

Use this command to set the interface or tunnel as nonpassive. It overrides the global passive mode that is currently effective on the interface or tunnel.

**Format**

no passive-interface {slot/port|vlan 1-4093|tunnel tunnel-id}

**Mode**

Router OSPFv3 Config

6.5.33 redistribute (OSPFv3)

This command configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

**Default**

- metric—unspecified
- type—2
- tag—0

**Format**

redistribute {static | connected} [metric 0-16777214] [metric-type {1 | 2}] [tag 0-4294967295]

**Mode**

Router OSPFv3 Config

6.5.33.1 no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

**Format**

no redistribute {static | connected} [metric] [metric-type] [tag]

**Mode**

Router OSPFv3 Config

6.5.34 router-id (OSPFv3)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The **ipaddress** is a configured value.

**Format**

router-id ipaddress

**Mode**

Router OSPFv3 Config

6.5.35 timers pacing lsa-group

Use this command to adjust how OSPFv3 groups LSAs for periodic refresh. OSPFv3 refreshes self-originated LSAs approximately once every 30 minutes. When OSPFv3 refreshes LSAs, it considers all self-originated LSAs whose age is from 1800 to 1800 plus the pacing group size. Grouping LSAs for refresh allows OSPFv3 to combine refreshed LSAs into a minimal number of LS Update packets. Minimizing the number of Update packets makes LSA distribution more efficient.

When OSPFv3 originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPFv3 refreshes the LSA. By selecting a random refresh delay, OSPFv3 avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.

**Default**

60 seconds

**Format**

timers pacing lsa-group seconds

**Mode**

Privileged EXEC
6.5.35.1 no timers pacing lsa-group

This command returns the LSA Group Pacing parameter to the factory default value of 60 seconds.

**Format**

no timers pacing lsa-group

**Mode**

Privileged EXEC

6.5.36 timers throttle spf

The initial “wait interval” is set to an amount of delay specified by the spf-hold value. If an SPF calculation is not scheduled during the current “wait interval”, the next SPF calculation is scheduled at a delay of spf-start. If there has been an SPF calculation scheduled during the current “wait interval”, the “wait interval” is set to two times the current “wait interval” until the “wait interval” reaches the maximum time in milliseconds as specified in spf-maximum. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.

**Default**

spf-start = 2000 ms
spf-hold = 5000 ms
spf-maximum = 5000 ms

**Format**

timers throttle spf spf-start spf-hold spf-maximum

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spf-start</td>
<td>Indicates the SPF schedule delay in milliseconds when no SPF calculation has been scheduled during the current “wait interval”. Value range is 1 to 600000 milliseconds.</td>
</tr>
<tr>
<td>spf-hold</td>
<td>Indicates the initial SPF “wait interval” in milliseconds. Value range is 1 to 600000 milliseconds.</td>
</tr>
<tr>
<td>spf-maximum</td>
<td>Indicates the maximum SPF “wait interval” in milliseconds. Value range is 1 to 600000 milliseconds.</td>
</tr>
</tbody>
</table>

6.5.36.1 no timers throttle spf

This command returns the SPF throttling parameters to the factory default values.

**Format**

no timers throttle spf

**Mode**

Privileged EXEC
6.5.37  trapflags (OSPFv3)

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group’s specific trapflags to enable or disable, are listed in Table 13.

Table 13:  Trapflag Groups (OSPFv3)

<table>
<thead>
<tr>
<th>Group</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>errors</td>
<td>•  authentication-failure</td>
</tr>
<tr>
<td></td>
<td>•  bad-packet</td>
</tr>
<tr>
<td></td>
<td>•  config-error</td>
</tr>
<tr>
<td></td>
<td>•  virt-authentication-failure</td>
</tr>
<tr>
<td></td>
<td>•  virt-bad-packet</td>
</tr>
<tr>
<td></td>
<td>•  virt-config-error</td>
</tr>
<tr>
<td>lsa</td>
<td>•  lsa-maxage</td>
</tr>
<tr>
<td></td>
<td>•  lsa-originate</td>
</tr>
<tr>
<td>overflow</td>
<td>•  lsdb-overflow</td>
</tr>
<tr>
<td></td>
<td>•  lsdb-approaching-overflow</td>
</tr>
<tr>
<td>retransmit</td>
<td>•  packets</td>
</tr>
<tr>
<td></td>
<td>•  virt-packets</td>
</tr>
<tr>
<td>state-change</td>
<td>•  if-state-change</td>
</tr>
<tr>
<td></td>
<td>•  neighbor-state-change</td>
</tr>
<tr>
<td></td>
<td>•  virtif-state-change</td>
</tr>
<tr>
<td></td>
<td>•  virtneighbor-state-change</td>
</tr>
</tbody>
</table>

- To enable the individual flag, enter the group name followed by that particular flag.
- To enable all the flags in that group, give the group name followed by all.
- To enable all the flags, give the command as trapflags all.

Default    enabled
Format      trapflags {
           | all |
           | errors {all | authentication-failure | bad-packet | config-error | virt-authentication-failure | virt-bad-packet | virt-config-error} |
           | lsa {all | lsa-maxage | lsa-originate} |
           | overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
           | retransmit {all | packets | virt-packets} |
           | state-change {all | if-state-change | neighbor-state-change | virtif-state-change | virtneighbor-state-change} }
Mode        Router OSPFv3 Config
6.5.37.1 no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the `group name` followed by that particular flag.
- To disable all the flags in that group, give the group name followed by `all`.
- To disable all the flags, give the command as `trapflags all`.

**Format**

```
no trapflags {
  all |
  errors {all | authentication-failure | bad-packet | config-error | virt-
            authentication-failure | virt-bad-packet | virt-config-error} |
  lsa {all | lsa-maxage | lsa-originate} |
  overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
  retransmit {all | packets | virt-packets} |
  state-change {all | if-state-change | neighbor-state-change | virtif-state-
               change | virtneighbor-state-change}
}
```

**Mode**

Router OSPFv3 Config

---

**OSPFv3 Interface Commands**

### 6.5.38 ipv6 ospf area

This command sets the OSPF area to which the specified router interface or range of interfaces belongs. It also enables OSPF on the specified router interface or range of interfaces. The `area` is a 32-bit integer, formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0-4294967295. The `area` uniquely identifies the area to which the interface connects. Assigning an area ID for an area that does not yet exist, causes the area to be created with default values.

**Format**

```
ipv6 ospf area 0-4294967295
```

**Mode**

Interface Config

### 6.5.39 ipv6 ospf cost

This command configures the cost on an OSPF interface or range of interfaces. The `cost` parameter has a range of 1 to 65535.

**Default**

10

**Format**

```
ipv6 ospf cost 1-65535
```

**Mode**

Interface Config
6.5.39.1  no ipv6 ospf cost
This command configures the default cost on an OSPF interface.

Format  no ipv6 ospf cost
Mode    Interface Config

6.5.40  ipv6 ospf dead-interval
This command sets the OSPF dead interval for the specified interface or range of interfaces. The value for seconds is a valid positive integer, which represents the length of time in seconds that a router’s Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e., 4). Valid values range for seconds is from 1 to 2147483647.

Format  ipv6 ospf dead-interval 1-2147483647
Mode    Interface Config

Default  40

6.5.40.1  no ipv6 ospf dead-interval
This command sets the default OSPF dead interval for the specified interface or range of interfaces.

Format  no ipv6 ospf dead-interval
Mode    Interface Config

6.5.41  ipv6 ospf hello-interval
This command sets the OSPF hello interval for the specified interface. The value for seconds is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network. Valid values for seconds range from 1 to 65535.

Default  10
Format  ipv6 ospf hello-interval seconds
Mode    Interface Config

6.5.41.1  no ipv6 ospf hello-interval
This command sets the default OSPF hello interval for the specified interface.

Format  no ipv6 ospf hello-interval
Mode    Interface Config
6.5.42  ipv6 ospf link-lsa-suppression

Use this command to enable Link LSA Suppression on an interface. When Link LSA Suppression is enabled on a point-to-point (P2P) interface, no Link LSA protocol packets are originated (transmitted) on the interface. This configuration does not apply to non-P2P interfaces.

Default     False
Format       ipv6 ospf link-lsa-suppression
Mode         Privileged EXEC

6.5.42.1 no ipv6 ospf link-lsa-suppression

This command returns Link LSA Suppression for the interface to disabled. When Link LSA Suppression is disabled, Link LSA protocol packets are originated (transmitted) on the P2P interface.

Format       no ipv6 ospf link-lsa-suppression
Mode         Privileged EXEC

6.5.43  ipv6 ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection on an interface or range of interfaces. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default     enabled
Format       ipv6 ospf mtu-ignore
Mode         Interface Config

6.5.43.1 no ipv6 ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format       no ipv6 ospf mtu-ignore
Mode         Interface Config

6.5.44  ipv6 ospf network

This command changes the default OSPF network type for the interface or range of interfaces. Normally, the network type is determined from the physical IP network type. By default all Ethernet networks are OSPF type broadcast. Similarly, tunnel interfaces default to point-to-point. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPF designated router election. It is normally not useful to set a tunnel to OSPF network type broadcast.

Default     broadcast
Format       ipv6 ospf network {broadcast | point-to-point}
Mode         Interface Config
6.5.44.1  no ipv6 ospf network
This command sets the interface type to the default value.

Format  no ipv6 ospf network {broadcast | point-to-point}
Mode    Interface Config

6.5.45  ipv6 ospf prefix-suppression
This command suppresses the advertisement of the IPv6 prefixes that are associated with an interface, except for those associated with secondary IPv6 addresses. This command takes precedence over the global configuration. If this configuration is not specified, the global prefix-suppression configuration applies.

prefix-suppression can be disabled at the interface level by using the disable option. The disable option is useful for excluding specific interfaces from performing prefix-suppression when the feature is enabled globally.

Note that the disable option disable is not equivalent to not configuring the interface specific prefix-suppression. If prefix-suppression is not configured at the interface level, the global prefix-suppression configuration is applicable for the IPv6 prefixes associated with the interface.

Default  prefix-suppression is not configured.
Format   ipv6 ospf prefix-suppression [disable]
Mode     Interface Config

6.5.45.1  no ipv6 ospf prefix-suppression
This command removes prefix-suppression configurations at the interface level. When the no ipv6 ospf prefix-suppression command is used, global prefix-suppression applies to the interface. Not configuring the command is not equal to disabling interface level prefix-suppression.

Format   no ipv6 ospf prefix-suppression
Mode     Interface Config

6.5.46  ipv6 ospf priority
This command sets the OSPF priority for the specified router interface or range of interfaces. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default  1, which is the highest router priority
Format   ipv6 ospf priority 0-255
Mode     Interface Config

6.5.46.1  no ipv6 ospf priority
This command sets the default OSPF priority for the specified router interface.

Format   no ipv6 ospf priority
Mode     Interface Config
6.5.47 ipv6 ospf retransmit-interval

This command sets the OSPF retransmit interval for the specified interface or range of interfaces. The retransmit interval is specified in seconds. The value for *seconds* is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

**Default**
5

**Format**
`ipv6 ospf retransmit-interval seconds`

**Mode**
Interface Config

6.5.47.1 no ipv6 ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

**Format**
`no ipv6 ospf retransmit-interval`

**Mode**
Interface Config

6.5.48 ipv6 ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface or range of interfaces. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for *seconds* range from 1 to 3600 (1 hour).

**Default**
1

**Format**
`ipv6 ospf transmit-delay seconds`

**Mode**
Interface Config

6.5.48.1 no ipv6 ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

**Format**
`no ipv6 ospf transmit-delay`

**Mode**
Interface Config

**OSPFv3 Graceful Restart Commands**

The OSPFv3 protocol can be configured to participate in the checkpointing service, so that these protocols can execute a "graceful restart" when the management unit fails. In a graceful restart, the hardware to continues forwarding IPv6 packets using OSPFv3 routes while a backup switch takes over management unit responsibility.

Graceful restart uses the concept of "helpful neighbors". A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. A planned restart is initiated by the operator through the management command `initiate failover`. The operator may initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.
6.5.49 nsf (OSPFv3)

Use this command to enable the OSPF graceful restart functionality on an interface. To disable graceful restart, use the no form of the command.

Default: Disabled

Format: nsf [ietf] [planned-only]

Modes: Router OSPFv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ietf</td>
<td>This keyword is accepted but not required.</td>
</tr>
<tr>
<td>planned-only</td>
<td>This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).</td>
</tr>
</tbody>
</table>

6.5.49.1 no nsf (OSPFv3)

Use this command to disable graceful restart for all restarts.

6.5.50 nsf restart-interval (OSPFv3)

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the initiate failover command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Default: 120 seconds

Format: nsf [ietf] restart-interval 1-1800

Modes: Router OSPFv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ietf</td>
<td>This keyword is accepted but not required.</td>
</tr>
<tr>
<td>seconds</td>
<td>The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.</td>
</tr>
</tbody>
</table>

6.5.50.1 no nsfrestart-interval (OSPFv3)

Use this command to revert the grace period to its default value.

Format: no [ietf] nsf restart-interval

Modes: Router OSPFv3 Config

6.5.51 nsf helper (OSPFv3)

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default: OSPF may act as a helpful neighbor for both planned and unplanned restarts

Format: nsf helper [planned-only]

Modes: Router OSPFv3 Config
6.5.51  no nsf helper (OSPFv3)

Use this command to disable helpful neighbor functionality for OSPF.

**Format**

```
no nsf helper
```

**Modes**

Router OSPFv3 Config

6.5.52  nsf ietf helper disable (OSPFv3)

Use this command to disable helpful neighbor functionality for OSPF.

**Format**

```
nsf ietf helper disable
```

**Modes**

Router OSPFv3 Config

---

**NOTICE**

The commands `no nsf helper` and `nsf ietf helper disable` are functionally equivalent. The command `nsf ietf helper disable` is supported solely for compatibility with other network software CLI.

---

6.5.53  nsf helper strict-lsa-checking (OSPFv3)

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router. A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

**Default**

Enabled.

**Format**

```
nsf [ietf] helper strict-lsa-checking
```

**Modes**

Router OSPFv3 Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ietf</td>
<td>This keyword is accepted but not required.</td>
</tr>
</tbody>
</table>
6.5.53.1 no nsf [ietf] helper strict-lsa-checking (OSPFv3)

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default: Enabled.

Format: nsf [ietf] helper strict-lsa-checking

Modes: Router OSPFv3 Config

OSPFv3 Stub Router Commands

6.5.54 max-metric router-lsa

To configure OSPFv3 to enter stub router mode, use this command in Router OSPFv3 Global Configuration mode. When OSPFv3 is in stub router mode, OSPFv3 sets the metric in the nonstub links in its router LSA to MaxLinkMetric. Other routers therefore compute very long paths through the stub router, and prefer any alternate path. Doing so eliminates all transit traffic through the stub router, when alternate routes are available. Stub router mode is useful when adding or removing a router from a network or to avoid transient routes when a router reloads.

You can administratively force OSPFv3 into stub router mode. OSPFv3 remains in stub router mode until you take OSPFv3 out of stub router mode. Alternatively, you can configure OSPF to start in stub router mode for a configurable period of time after the router boots up.

If you set the summary LSA metric to 16,777,215, other routers will skip the summary LSA when they compute routes.

If you have configured the router to enter stub router mode on startup (max-metric router-lsa on-startup), and then enter max-metric router lsa, there is no change. If OSPFv3 is administratively in stub router mode (the max-metric router-lsa command has been given), and you configure OSPFv3 to enter stub router mode on startup (max-metric router-lsa on-startup), OSPFv3 exits stub router mode (assuming the startup period has expired) and the configuration is updated. Without any parameters, stub router mode only sends maximum metric values for router LSAs.

Default: OSPF is not in stub router mode by default

Format:
max-metric router-lsa [on-startup seconds] [summary-lsa {metric}]

max-metric router-lsa [external-lsa [max-metric-value]] [inter-area-lsas [max-metric-value]] [on-startup seconds] [summary-lsa [max-metric-value]]

Mode: OSPFv3 Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>external-lsa</td>
<td>(Optional) Sends the maximum metric values for external LSAs. max-metric-value is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFF). The default value is 16711680 (0xFF0000).</td>
</tr>
<tr>
<td>inter-area-lsas</td>
<td>(Optional) Sends the maximum metric values for Inter-Area-Router LSAs</td>
</tr>
<tr>
<td>on-startup</td>
<td>(Optional) Starts OSPF in stub router mode. seconds is the number of seconds that OSPF remains in stub router mode after a reboot. The range is 5 to 86,400 seconds. There is no default value.</td>
</tr>
<tr>
<td>summary-lsa</td>
<td>(Optional) Sends the maximum metric values for Summary LSAs</td>
</tr>
</tbody>
</table>
6.5.54.1 no max-metric router-lsa

Use this command in OSPFv3 Router Configuration mode to disable stub router mode. The command clears either type of stub router mode (always or on-startup) and resets all LSA options. If OSPF is configured to enter global configuration mode on startup, and during normal operation you want to immediately place OSPF in stub router mode, issue the command no max-metric router-lsa on-startup. The command no max-metric with the external-lsa, inter-area-lsas, or summary-lsa option router-lsa summary-lsa causes OSPF to send summary LSAs with metrics computed using normal procedures.

Format
no max-metric router-lsa [external-lsa] [inter-area-lsas] [on-startup] [summary-lsa]

Mode
OSPFv3 Router Configuration

6.5.55 clear ipv6 ospf stub-router

Use this command to force OSPF to exit stub router mode when it has automatically entered stub router mode because of a resource limitation. OSPF only exits stub router mode if it entered stub router mode because of a resource limitation or if it is in stub router mode at startup. This command has no effect if OSPF is configured to be in stub router mode permanently.

Format
clear ipv6 ospf stub-router

Mode
Privileged EXEC

OSPFv3 Show Commands

6.5.56 show ipv6 ospf

This command displays information relevant to the OSPF router.

Format
show ipv6 ospf

Mode
• Privileged EXEC
• User EXEC

NOTICE
Some of the information below displays only if you enable OSPF and configure certain features.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.</td>
</tr>
<tr>
<td>External LSDB Limit</td>
<td>The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.</td>
</tr>
<tr>
<td>Exit Overflow Interval</td>
<td>The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.</td>
</tr>
<tr>
<td>SPF Start Time</td>
<td>The number of milliseconds the SPF calculation is delayed if no SPF calculation has been scheduled during the current &quot;wait interval&quot;.</td>
</tr>
<tr>
<td>SPF Hold Time</td>
<td>The number of milliseconds of the initial &quot;wait interval&quot;.</td>
</tr>
<tr>
<td>SPF Maximum Hold Time</td>
<td>The maximum number of milliseconds of the &quot;wait interval&quot;.</td>
</tr>
<tr>
<td>LSA Refresh Group Pacing Time</td>
<td>The size of the LSA refresh group window, in seconds.</td>
</tr>
<tr>
<td>AutoCost Ref BW</td>
<td>Shows the value of the auto-cost reference bandwidth configured on the router.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Passive Setting</td>
<td>Shows whether the interfaces are passive by default.</td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>The maximum number of paths that OSPF can report for a given destination.</td>
</tr>
<tr>
<td>Default Metric</td>
<td>Default value for redistributed routes.</td>
</tr>
<tr>
<td>Default Route Advertise</td>
<td>Indicates whether the default routes received from other source protocols are advertised or not.</td>
</tr>
<tr>
<td>Always</td>
<td>Shows whether default routes are always advertised.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric for the advertised default routes. If the metric is not configured, this field is blank.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>Shows whether the routes are External Type 1 or External Type 2.</td>
</tr>
<tr>
<td>Number of Active Areas</td>
<td>The number of active OSPF areas. An “active” OSPF area is an area with at least one interface up.</td>
</tr>
<tr>
<td>ABR Status</td>
<td>Shows whether the router is an OSPF Area Border Router.</td>
</tr>
<tr>
<td>ASBR Status</td>
<td>Shows if the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).</td>
</tr>
<tr>
<td>Stub Router Status</td>
<td>The status of the stub router: Active or Inactive.</td>
</tr>
<tr>
<td>Stub Router Reason</td>
<td>This is displayed only if the stub router is active. Shows the reason for the stub router: Configured, Startup, or Resource Limitation</td>
</tr>
<tr>
<td>Stub Router Startup Time</td>
<td>This is displayed only if the stub router is in startup stub router mode. The remaining time (in seconds) until OSPF exits stub router mode.</td>
</tr>
<tr>
<td>Stub Router Duration</td>
<td>This row is only listed if the stub router is active and the router entered stub mode because of a resource limitation. The time elapsed since the router last entered the stub router mode. The duration is displayed in DD:HH:MM:SS format.</td>
</tr>
<tr>
<td>External LSDB Overflow</td>
<td>When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.</td>
</tr>
<tr>
<td>External LSA Count</td>
<td>The number of external (LS type 5) link-state advertisements in the link-state database.</td>
</tr>
<tr>
<td>External LSA Checksum</td>
<td>The sum of the LS checksums of external link-state advertisements contained in the link-state database.</td>
</tr>
<tr>
<td>New LSAs Originated</td>
<td>The number of new link-state advertisements that have been originated.</td>
</tr>
<tr>
<td>LSA Count</td>
<td>The total number of link state advertisements currently in the link state database.</td>
</tr>
<tr>
<td>Maximum Number of LSAs</td>
<td>The maximum number of LSAs that OSPF can store.</td>
</tr>
<tr>
<td>LSA High Water Mark</td>
<td>The maximum size of the link state database since the system started.</td>
</tr>
<tr>
<td>Retransmit List Entries</td>
<td>The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.</td>
</tr>
<tr>
<td>Maximum Number of Retransmit Entries</td>
<td>The maximum number of LSAs that can be waiting for acknowledgment at any given time.</td>
</tr>
<tr>
<td>Retransmit Entries High Water Mark</td>
<td>The highest number of LSAs that have been waiting for acknowledgment.</td>
</tr>
<tr>
<td>Redistributing</td>
<td>This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.</td>
</tr>
</tbody>
</table>
6.5.57  show ipv6 ospf abr

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR). This command takes no options.

**Format**

```
show ipv6 ospf abr
```

**Modes**

- Privileged EXEC
- User EXEC

### Term | Definition

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
<td>Shows source protocol/routes that are being redistributed. Possible values are static, connected or RIP.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>The metric of the routes being redistributed.</td>
</tr>
<tr>
<td><strong>Metric Type</strong></td>
<td>Shows whether the routes are External Type 1 or External Type 2.</td>
</tr>
<tr>
<td><strong>Tag</strong></td>
<td>The decimal value attached to each external route.</td>
</tr>
<tr>
<td><strong>Subnets</strong></td>
<td>For redistributing routes into OSPF, the scope of redistribution for the specified protocol.</td>
</tr>
<tr>
<td><strong>Distribute-List</strong></td>
<td>The access list used to filter redistributed routes.</td>
</tr>
<tr>
<td><strong>Prefix-suppression</strong></td>
<td>Displays whether prefix-suppression is enabled or disabled on the given interface.</td>
</tr>
<tr>
<td><strong>NSF Support</strong></td>
<td>Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (Always).</td>
</tr>
<tr>
<td><strong>NSF Restart Interval</strong></td>
<td>The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.</td>
</tr>
<tr>
<td><strong>NSF Restart Status</strong></td>
<td>The current graceful restart status of the router.</td>
</tr>
<tr>
<td><strong>NSF Restart Age</strong></td>
<td>Number of seconds until the graceful restart grace period expires.</td>
</tr>
<tr>
<td><strong>NSF Restart Exit Reason</strong></td>
<td>Indicates why the router last exited the last restart:</td>
</tr>
<tr>
<td></td>
<td>• None — Graceful restart has not been attempted.</td>
</tr>
<tr>
<td></td>
<td>• In Progress — Restart is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Completed — The previous graceful restart completed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Timed Out — The previous graceful restart timed out.</td>
</tr>
<tr>
<td></td>
<td>• Topology Changed — The previous graceful restart terminated prematurely because of a topology change.</td>
</tr>
<tr>
<td><strong>NSF Help Support</strong></td>
<td>Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).</td>
</tr>
<tr>
<td><strong>NSF help Strict LSA checking</strong></td>
<td>Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.</td>
</tr>
</tbody>
</table>

**Term | Definition**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>The type of the route to the destination. It can be either:</td>
</tr>
<tr>
<td></td>
<td>• intra — Intra-area route</td>
</tr>
<tr>
<td></td>
<td>• inter — Inter-area route</td>
</tr>
<tr>
<td><strong>Router ID</strong></td>
<td>Router ID of the destination.</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Cost of using this route.</td>
</tr>
<tr>
<td><strong>Area ID</strong></td>
<td>The area ID of the area from which this route is learned.</td>
</tr>
<tr>
<td><strong>Next Hop</strong></td>
<td>Next hop toward the destination.</td>
</tr>
<tr>
<td><strong>Next Hop Intf</strong></td>
<td>The outgoing router interface to use when forwarding traffic to the next hop.</td>
</tr>
</tbody>
</table>
6.5.58  show ipv6 ospf area

This command displays information about the area. The areaid identifies the OSPF area that is being displayed.

Format: show ipv6 ospf area areaid
Modes: • Privileged EXEC
        • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AreaID</td>
<td>The area id of the requested OSPF area.</td>
</tr>
<tr>
<td>External Routing</td>
<td>A number representing the external routing capabilities for this area.</td>
</tr>
<tr>
<td>Spf Runs</td>
<td>The number of times that the intra-area route table has been calculated using this area's link-state database.</td>
</tr>
<tr>
<td>Area Border Router Count</td>
<td>The total number of area border routers reachable within this area.</td>
</tr>
<tr>
<td>Area LSA Count</td>
<td>Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.</td>
</tr>
<tr>
<td>Area LSA Checksum</td>
<td>A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.</td>
</tr>
<tr>
<td>Stub Mode</td>
<td>Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.</td>
</tr>
<tr>
<td>Import Summary LSAs</td>
<td>Shows whether to import summary LSAs (enabled).</td>
</tr>
<tr>
<td>OSPF Stub Metric Value</td>
<td>The metric value of the stub area. This field displays only if the area is a configured as a stub area.</td>
</tr>
</tbody>
</table>

The following OSPF NSSA specific information displays only if the area is configured as an NSSA.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Summary LSAs</td>
<td>Shows whether to import summary LSAs into the NSSA.</td>
</tr>
<tr>
<td>Redistribute into NSSA</td>
<td>Shows whether to redistribute information into the NSSA.</td>
</tr>
<tr>
<td>Default Information Originate</td>
<td>Shows whether to advertise a default route into the NSSA.</td>
</tr>
<tr>
<td>Default Metric</td>
<td>The metric value for the default route advertised into the NSSA.</td>
</tr>
<tr>
<td>Default Metric Type</td>
<td>The metric type for the default route advertised into the NSSA.</td>
</tr>
<tr>
<td>Translator Role</td>
<td>The NSSA translator role of the ABR, which is always or candidate.</td>
</tr>
<tr>
<td>Translator Stability Interval</td>
<td>The amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.</td>
</tr>
<tr>
<td>Translator State</td>
<td>Shows whether the ABR translator state is disabled, always, or elected.</td>
</tr>
</tbody>
</table>

6.5.59  show ipv6 ospf asbr

This command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routers (ASBR). This command takes no options.

Format: show ipv6 ospf asbr
Modes: • Privileged EXEC
        • User EXEC
6.5.60  show ipv6 ospf database

This command displays information about the link state database when OSPFv3 is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional areaid parameter to display database information about a specific area. Use the other optional parameters to specify the type of link state advertisements to display. Use external to display the external LSAs. Use inter-area to display the inter-area LSAs. Use link to display the link LSAs. Use network to display the network LSAs. Use nssa-external to display NSSA external LSAs. Use prefix to display intra-area Prefix LSAs. Use router to display router LSAs. Use unknown area, unknown as, or unknown link to display unknown area, AS or link-scope LSAs, respectively. Use lsid to specify the link state ID (LSID). Use adv-router to show the LSAs that are restricted by the advertising router. Use self-originated to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled.

Format  show ipv6 ospf [areaid] database [{external | inter-area} {prefix | router} | link | network | nssa-external | prefix | router | unknown {area | as | link})] [lsid] [{adv-router [rtrid] | self-originated}]

Modes  • Privileged EXEC
• User EXEC

For each link-type and area, the following information is displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Id</td>
<td>A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.</td>
</tr>
<tr>
<td>Adv Router</td>
<td>The Advertising Router. Is a 32-bit dotted decimal number representing the LSDB interface.</td>
</tr>
<tr>
<td>Age</td>
<td>A number representing the age of the link state advertisement in seconds.</td>
</tr>
<tr>
<td>Sequence</td>
<td>A number that represents which LSA is more recent.</td>
</tr>
<tr>
<td>Checksum</td>
<td>The total number LSA checksum.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The IPv6 prefix.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface for the link.</td>
</tr>
<tr>
<td>Rtr Count</td>
<td>The number of routers attached to the network.</td>
</tr>
</tbody>
</table>

6.5.61  show ipv6 ospf database database-summary

Use this command to display the number of each type of LSA in the database and the total number of LSAs in the database.

Format  show ipv6 ospf database database-summary

Modes  • Privileged EXEC
• User EXEC
### 6.5.62 `show ipv6 ospf interface`

This command displays the information for the IFO object or virtual interface tables. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a `slot/port` format.

**Format**

```
show ipv6 ospf interface {slot/port|vlan 1-4093|loopback loopback-id | tunnel tunnel-id}
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>The IPv6 address of the interface.</td>
</tr>
<tr>
<td>iIfIndex</td>
<td>The interface index number associated with the interface.</td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>Shows whether the admin mode is enabled or disabled.</td>
</tr>
<tr>
<td>OSPF Area ID</td>
<td>The area ID associated with this interface.</td>
</tr>
<tr>
<td>Router Priority</td>
<td>The router priority. The router priority determines which router is the designated router.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>The frequency, in seconds, at which the interface sends LSA.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The frequency, in seconds, at which the interface sends Hello packets.</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>The amount of time, in seconds, the interface waits before assuming a neighbor is down.</td>
</tr>
<tr>
<td>LSA Ack Interval</td>
<td>The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.</td>
</tr>
<tr>
<td>Interface Transmit Delay</td>
<td>The number of seconds the interface adds to the age of LSA packets before transmission.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The type of authentication the interface performs on LSAs it receives.</td>
</tr>
<tr>
<td>Metric Cost</td>
<td>The priority of the path. Low costs have a higher priority than high costs.</td>
</tr>
<tr>
<td>Prefix-suppression</td>
<td>Displays whether prefix-suppression is enabled, disabled, or unconfigured on the given interface.</td>
</tr>
<tr>
<td>Passive Status</td>
<td>Shows whether the interface is passive or not.</td>
</tr>
<tr>
<td>OSPF MTU-ignore</td>
<td>Shows whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.</td>
</tr>
<tr>
<td>Link LSA Suppression</td>
<td>The configured state of Link LSA Suppression for the interface.</td>
</tr>
</tbody>
</table>
The following information only displays if OSPF is initialized on the interface:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OSPF Interface Type</strong></td>
<td>Broadcast LANs, such as Ethernet and IEEE 802.5, take the value <em>broadcast</em>. The OSPF Interface Type will be 'broadcast'.</td>
</tr>
<tr>
<td>State</td>
<td>The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>The router ID representing the designated router.</td>
</tr>
<tr>
<td>Backup Designated Router</td>
<td>The router ID representing the backup designated router.</td>
</tr>
<tr>
<td>Number of Link Events</td>
<td>The number of link events.</td>
</tr>
<tr>
<td>Metric Cost</td>
<td>The cost of the OSPF interface.</td>
</tr>
</tbody>
</table>

**6.5.63 show ipv6 ospf interface brief**

This command displays brief information for the IFO object or virtual interface tables.

**Format**

```
show ipv6 ospf interface brief
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td><em>slot/port</em></td>
</tr>
<tr>
<td>OSPF Admin Mode</td>
<td>States whether OSPF is enabled or disabled on a router interface.</td>
</tr>
<tr>
<td>OSPF Area ID</td>
<td>The OSPF Area ID for the specified interface.</td>
</tr>
<tr>
<td>Router Priority</td>
<td>The router priority. The router priority determines which router is the designated router.</td>
</tr>
<tr>
<td>Metric Cost</td>
<td>The priority of the path. Low costs have a higher priority than high costs.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The frequency, in seconds, at which the interface sends Hello packets.</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>The amount of time, in seconds, the interface waits before assuming a neighbor is down.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>The frequency, in seconds, at which the interface sends LSA.</td>
</tr>
<tr>
<td>Retransmit Delay Interval</td>
<td>The number of seconds the interface adds to the age of LSA packets before transmission.</td>
</tr>
<tr>
<td>LSA Ack Interval</td>
<td>The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.</td>
</tr>
</tbody>
</table>

**6.5.64 show ipv6 ospf interface stats**

This command displays the statistics for a specific interface. The command displays information only if OSPF is enabled.

**Format**

```
show ipv6 ospf interface stats slot/port
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3 Area ID</td>
<td>The area id of this OSPF interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address associated with this OSPF interface.</td>
</tr>
<tr>
<td>OSPFv3 Interface Events</td>
<td>The number of times the specified OSPF interface has changed its state, or an error has occurred.</td>
</tr>
<tr>
<td>Virtual Events</td>
<td>The number of state changes or errors that occurred on this virtual link.</td>
</tr>
</tbody>
</table>
Table 11 on page 602 lists the number of OSPF packets of each type sent and received on the interface.

### 6.5.65 show ipv6 ospf lsa-group

This command displays the number of self-originated LSAs within each LSA group.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total self-originated LSAs</td>
<td>The number of LSAs the router is currently originating.</td>
</tr>
<tr>
<td>Average LSAs per group</td>
<td>The number of self-originated LSAs divided by the number of LSA groups. The number of LSA groups is the refresh interval (1800 seconds) divided by the pacing interval (configured with timers pacing lsa-group) plus two.</td>
</tr>
<tr>
<td>Pacing group limit</td>
<td>The maximum number of self-originated LSAs in one LSA group. If the number of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout the refresh interval to achieve better balance.</td>
</tr>
<tr>
<td>Groups</td>
<td>For each LSA pacing group, the output shows the range of LSA ages in the group and the number of LSAs in the group.</td>
</tr>
</tbody>
</table>
**Example:** The following shows an example of the command.

(R1) #show ipv6 ospf lsa-group

Total self-originated LSAs: 3019
Average LSAs per group: 100
Pacing group limit: 400
Number of self-originated LSAs within each LSA group...

<table>
<thead>
<tr>
<th>Group Start Age</th>
<th>Group End Age</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>59</td>
<td>96</td>
</tr>
<tr>
<td>60</td>
<td>119</td>
<td>88</td>
</tr>
<tr>
<td>120</td>
<td>179</td>
<td>102</td>
</tr>
<tr>
<td>180</td>
<td>239</td>
<td>95</td>
</tr>
<tr>
<td>240</td>
<td>299</td>
<td>95</td>
</tr>
<tr>
<td>300</td>
<td>359</td>
<td>92</td>
</tr>
<tr>
<td>360</td>
<td>419</td>
<td>48</td>
</tr>
<tr>
<td>420</td>
<td>479</td>
<td>58</td>
</tr>
<tr>
<td>480</td>
<td>539</td>
<td>103</td>
</tr>
<tr>
<td>540</td>
<td>599</td>
<td>99</td>
</tr>
<tr>
<td>600</td>
<td>659</td>
<td>119</td>
</tr>
<tr>
<td>660</td>
<td>719</td>
<td>110</td>
</tr>
<tr>
<td>720</td>
<td>779</td>
<td>106</td>
</tr>
<tr>
<td>780</td>
<td>839</td>
<td>122</td>
</tr>
<tr>
<td>840</td>
<td>899</td>
<td>110</td>
</tr>
<tr>
<td>900</td>
<td>959</td>
<td>99</td>
</tr>
<tr>
<td>960</td>
<td>1019</td>
<td>135</td>
</tr>
<tr>
<td>1020</td>
<td>1079</td>
<td>101</td>
</tr>
<tr>
<td>1080</td>
<td>1139</td>
<td>94</td>
</tr>
<tr>
<td>1140</td>
<td>1199</td>
<td>115</td>
</tr>
<tr>
<td>1200</td>
<td>1259</td>
<td>110</td>
</tr>
<tr>
<td>1260</td>
<td>1319</td>
<td>111</td>
</tr>
<tr>
<td>1320</td>
<td>1379</td>
<td>111</td>
</tr>
<tr>
<td>1380</td>
<td>1439</td>
<td>99</td>
</tr>
<tr>
<td>1440</td>
<td>1499</td>
<td>102</td>
</tr>
<tr>
<td>1500</td>
<td>1559</td>
<td>96</td>
</tr>
<tr>
<td>1560</td>
<td>1619</td>
<td>106</td>
</tr>
<tr>
<td>1620</td>
<td>1679</td>
<td>111</td>
</tr>
<tr>
<td>1680</td>
<td>1739</td>
<td>106</td>
</tr>
<tr>
<td>1740</td>
<td>1799</td>
<td>80</td>
</tr>
<tr>
<td>1800</td>
<td>1859</td>
<td>0</td>
</tr>
<tr>
<td>1860</td>
<td>1919</td>
<td>0</td>
</tr>
</tbody>
</table>

### 6.5.66 show ipv6 ospf max-metric

This command displays the configured maximum metrics for stub-router mode.

**Format**

```
show ipv6 ospf max-metric
```

**Modes**

- Privileged EXEC
- User EXEC

**Example:** The following shows an example of the command.

(config)#show ipv6 ospf max-metric

OSPFv3 Router with ID (3.3.3.3)
Start time: 00:00:00, Time elapsed: 00:01:05
Originating router-LSAs with maximum metric
Condition: on startup for 1000 seconds, State: inactive
Advertise external-LSAs with metric 16711680

---
6.5.67  show ipv6 ospf neighbor

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays. The argument \texttt{slot/port} corresponds to a physical routing interface or VLAN routing interface. The keyword \texttt{vlan} is used to specify the VLAN ID of the routing VLAN directly instead of a \texttt{slot/port} format. The \texttt{ip-address} is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

**Format**

\texttt{show ipv6 ospf neighbor [interface \{slot/port|vlan 1-4093|tunnel tunnel_id\}][ip-address]}

**Modes**

\begin{itemize}
  \item Privileged EXEC
  \item User EXEC
\end{itemize}

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The 4-digit dotted-decimal number of the neighbor router.</td>
</tr>
<tr>
<td>Priority</td>
<td>The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.</td>
</tr>
<tr>
<td>Intf ID</td>
<td>The interface ID of the neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface of the local router in \texttt{slot/port} format.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the neighboring routers. Possible values are:</td>
</tr>
</tbody>
</table>
|              | \begin{itemize}
  \item Down - initial state of the neighbor conversation - no recent information has been received from the neighbor.
  \item Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.
  \item Init - an Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established.
  \item 2 way - communication between the two routers is bidirectional.
  \item Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.
  \item Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor.
  \item Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
\end{itemize} |
| Dead Time    | The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable. |
| Restart Helper Status | Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: |
|              | \begin{itemize}
  \item Helping—This router is acting as a helpful neighbor to the specified router.
  \item Not Helping—This router is not a helpful neighbor at this time.
\end{itemize} |
| Restart Reason | When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router. |
| Remaining Grace Time | The number of seconds remaining in the current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command. |
If you specify an IP address for the neighbor router, the following fields display:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface of the local router in slot/port format.</td>
</tr>
<tr>
<td>Area ID</td>
<td>The area ID associated with the interface.</td>
</tr>
<tr>
<td>Options</td>
<td>An integer value that indicates the optional OSPF capabilities supported by the neighbor. These are listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.</td>
</tr>
<tr>
<td>Router Priority</td>
<td>The router priority for the specified interface.</td>
</tr>
<tr>
<td>Dead Timer Due</td>
<td>The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the neighboring routers.</td>
</tr>
<tr>
<td>Events</td>
<td>Number of times this neighbor relationship has changed state, or an error has occurred.</td>
</tr>
<tr>
<td>Retransmission Queue Length</td>
<td>An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.</td>
</tr>
</tbody>
</table>

6.5.68  show ipv6 ospf range

This command displays the set of OSPFv3 area ranges configured for a given area.

Format  show ipv6 ospf range areaid

Modes  Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>The area whose prefixes are summarized.</td>
</tr>
<tr>
<td>IPv6 Prefix/Prefix Length</td>
<td>The summary prefix and prefix length.</td>
</tr>
<tr>
<td>Type</td>
<td>S (Summary Link) or E (External Link)</td>
</tr>
<tr>
<td>Action</td>
<td>Enabled or Disabled</td>
</tr>
<tr>
<td>Cost</td>
<td>Metric to be advertised when the range is active.</td>
</tr>
</tbody>
</table>

6.5.69  show ipv6 ospf statistics

This command displays information about the 15 most recent Shortest Path First (SPF) calculations. SPF is the OSPF routing table calculation.

Format  show ipv6 ospf statistics

Modes  • Privileged EXEC
        • User EXEC
The command displays the following information with the most recent statistics displayed at the end of the table.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delta T</td>
<td>The time since the routing table was computed. The time is in the format hours, minutes, and seconds (hh:mm:ss).</td>
</tr>
<tr>
<td>Intra</td>
<td>The time taken to compute intra-area routes, in milliseconds.</td>
</tr>
<tr>
<td>Summ</td>
<td>The time taken to compute inter-area routes, in milliseconds.</td>
</tr>
<tr>
<td>Ext</td>
<td>The time taken to compute external routes, in milliseconds.</td>
</tr>
<tr>
<td>SPF Total</td>
<td>The total time taken to compute routes, in milliseconds. The total may exceed the sum of Intra, Summ, and Ext times.</td>
</tr>
<tr>
<td>RIB Update</td>
<td>The time from the completion of the routing table calculation until all changes have been made in the common routing table [the Routing Information Base (RIB)], in milliseconds.</td>
</tr>
<tr>
<td>Reason</td>
<td>The event or events that triggered the SPF. The reason codes are as follows:</td>
</tr>
<tr>
<td></td>
<td>• R: New router LSA</td>
</tr>
<tr>
<td></td>
<td>• N: New network LSA</td>
</tr>
<tr>
<td></td>
<td>• SN: New network (inter-area prefix) summary LSA</td>
</tr>
<tr>
<td></td>
<td>• SA: New ASBR (inter-area router) summary LSA</td>
</tr>
<tr>
<td></td>
<td>• X: New external LSA</td>
</tr>
<tr>
<td></td>
<td>• IP: New intra-area prefix LSA</td>
</tr>
<tr>
<td></td>
<td>• L: New Link LSA</td>
</tr>
</tbody>
</table>

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

(Routing) #show ipv6 ospf statistics

Area 0.0.0.0: SPF algorithm executed 10 times

<table>
<thead>
<tr>
<th>Delta T</th>
<th>Intra</th>
<th>Summ</th>
<th>Ext</th>
<th>SPF Total</th>
<th>RIB Update</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>23:32:46</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R, IP</td>
</tr>
<tr>
<td>23:32:09</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R, N, IP</td>
</tr>
<tr>
<td>23:32:04</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R</td>
</tr>
<tr>
<td>23:31:44</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>R, N, IP</td>
</tr>
<tr>
<td>23:31:39</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>R</td>
</tr>
<tr>
<td>23:29:57</td>
<td>0</td>
<td>3</td>
<td>7</td>
<td>10</td>
<td>131</td>
<td>R</td>
</tr>
<tr>
<td>23:29:52</td>
<td>0</td>
<td>14</td>
<td>29</td>
<td>43</td>
<td>568</td>
<td>SN</td>
</tr>
<tr>
<td>04:07:23</td>
<td>0</td>
<td>9</td>
<td>23</td>
<td>33</td>
<td>117</td>
<td>SN</td>
</tr>
<tr>
<td>04:07:23</td>
<td>0</td>
<td>9</td>
<td>23</td>
<td>33</td>
<td>117</td>
<td>SN</td>
</tr>
<tr>
<td>04:07:18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>485</td>
<td>SN</td>
</tr>
<tr>
<td>04:07:14</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>X</td>
</tr>
</tbody>
</table>

**6.5.70 show ipv6 ospf stub table**

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

**Format**  
show ipv6 ospf stub table

**Modes**  
• Privileged EXEC  
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>A 32-bit identifier for the created stub area.</td>
</tr>
<tr>
<td>Type of Service</td>
<td>Type of service associated with the stub metric. For this release, Normal TOS is the only supported type.</td>
</tr>
</tbody>
</table>
6.5.71  show ipv6 ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The areaid parameter identifies the area and the neighbor parameter identifies the neighbor’s Router ID.

Format  
```
show ipv6 ospf virtual-link areaid neighbor
```

Modes  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric Value</td>
<td>The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.</td>
</tr>
<tr>
<td>Import Summary LSA</td>
<td>Controls the import of summary LSAs into stub areas.</td>
</tr>
</tbody>
</table>

6.5.72  show ipv6 ospf virtual-link brief

This command displays the OSPFV3 Virtual Interface information for all areas in the system.

Format  
```
show ipv6 ospf virtual-link brief
```

Modes  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>The area id of the requested OSPFV3 area.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>The neighbor interface of the OSPFV3 virtual interface.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The configured hello interval for the OSPFV3 virtual interface.</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>The configured dead interval for the OSPFV3 virtual interface.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>The configured retransmit interval for the OSPFV3 virtual interface.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The type of authentication the interface performs on LSAs it receives.</td>
</tr>
<tr>
<td>State</td>
<td>The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.</td>
</tr>
<tr>
<td>Neighbor State</td>
<td>The neighbor state.</td>
</tr>
</tbody>
</table>
6.6 DHCPv6 Commands
This section describes the commands you use to configure the DHCPv6 server on the system and to view DHCPv6 information.

6.6.1 service dhcpv6
This command enables DHCPv6 configuration on the router.

**Default** enabled
**Format** service dhcpv6
**Mode** Global Config

6.6.1.1 no service dhcpv6
This command disables DHCPv6 configuration on router.

**Format** no service dhcpv6
**Mode** Global Config

6.6.2 ipv6 dhcp client pd
Use this command to enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process (if the process is not currently running) and to enable requests for prefix delegation through a specified interface. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the automatic argument.

**NOTICE**
The Prefix Delegation client is supported on only one IP interface.

**rapid-commit** enables the use of a two-message exchange method for prefix delegation and other configuration. If enabled, the client includes the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. If one of these functions is already enabled and a user tries to configure a different function on the same interface, a message is displayed.

**Default** Prefix delegation is disabled on an interface.
**Format** ipv6 dhcp client pd [rapid-commit]
**Mode** Interface Config

**Example**: The following examples enable prefix delegation on interface 0/1:
```
(Switch) #configure
(Switch) (Config)#interface 0/1
(Switch) (Interface 0/1)# ipv6 dhcp client pd

(Switch) #configure
(Switch) (Config)#interface 0/1
(Switch) (Interface 0/1)# ipv6 dhcp client pd rapid-commit
```
6.6.2.1  **no ipv6 dhcp client pd**
This command disables requests for prefix delegation.

**Format**

```
no ipv6 dhcp client pd
```

**Mode**

Interface Config

6.6.3  **ipv6 dhcp server**
Use this command to configure DHCPv6 server functionality on an interface or range of interfaces. The **pool-name** is the DHCPv6 pool containing stateless and/or prefix delegation parameters. **automatic** enables the server to automatically determine which pool to use when allocating addresses for a client. **rapid-commit** is an option that allows for an abbreviated exchange between the client and server, and **pref-value** is a value used by clients to determine preference between multiple DHCPv6 servers. For a particular interface, DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

**Format**

```
ipv6 dhcp server {pool-name | automatic}[rapid-commit] [preference pref-value]
```

**Mode**

Interface Config

6.6.4  **ipv6 dhcp relay destination**
Use this command to configure an interface for DHCPv6 relay functionality on an interface or range of interfaces. Use the **destination** keyword to set the relay server IPv6 address. The **relay-address** parameter is an IPv6 address of a DHCPv6 relay server. Use the **interface** keyword to set the relay server interface. The **relay-interface** parameter is an interface (slot/port) to reach a relay server. The optional **remote-id** is the Relay Agent Information Option "remote ID" suboption to be added to relayed messages. This can either be the special keyword **duid-ifid**, which causes the "remote ID" to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

---

**NOTICE**
If relay-address is an IPv6 global address, then relay-interface is not required. If relay-address is a link-local or multicast address, then relay-interface is required. Finally, if you do not specify a value for relay-address, then you must specify a value for relay-interface and the DHCPv6-ALL-AGENTS multicast address (i.e. FF02::1:2) is used to relay DHCPv6 messages to the relay server.

---

**Format**

```
ipv6 dhcp relay {destination [relay-address] interface [relay-interface][relay-interface][remote-id (duid-ifid | user-defined-string)]
```

**Mode**

Interface Config

6.6.5  **ipv6 dhcp relay remote-id**
This command configures the relay agent information option **remote ID** sub-option to be added to the DHCPv6 relayed messages. This can either be the special keyword **duid-ifid**, which causes the remote ID to be derived from the DHCPv6 Server DUID and the relay interface number, or it can be specified as a user-defined string.

**Default**

None configured

**Format**

```
ipv6 dhcp relay remote-id {duid-ifid | user-defined-string}
```

**Mode**

Interface Config
6.6.5.1 **no ipv6 dhcp relay remote-id**

This command resets the relay agent information option remote ID sub-option to be added to the DHCPv6 relayed messages to the default value.

- **Default**: None configured
- **Format**: `no ipv6 dhcp relay remote-id {duid-ifid | user-defined-string})`
- **Mode**: Interface Config

---

6.6.6 **ipv6 dhcp pool**

Use this command from Global Config mode to enter IPv6 DHCP Pool Config mode. Use the `exit` command to return to Global Config mode. To return to the User EXEC mode, enter CTRL+Z. The `pool-name` should be less than 31 alphanumeric characters. DHCPv6 pools are used to specify information for DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

Once the DHCP for IPv6 configuration information pool has been created, use the `ipv6 dhcp server` command to associate the pool with a server on an interface. If you do not configure an information pool, use the `ipv6 dhcp server interface` configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface. Not using any IPv6 address prefix means that the pool returns only configured options.

- **Format**: `ipv6 dhcp pool pool-name`
- **Mode**: Global Config

---

6.6.6.1 **no ipv6 dhcp pool**

This command removes the specified DHCPv6 pool.

- **Format**: `no ipv6 dhcp pool pool-name`
- **Mode**: Global Config

---

6.6.7 **address prefix (IPv6)**

Use this command to sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.

If `lifetime` values are not configured, the default lifetime values for `valid-lifetime` and `preferred-lifetime` are considered to be infinite.

- **Format**: `address prefix ipv6-prefix [lifetime {valid-lifetime preferred-lifetime | infinite}]`
- **Mode**: IPv6 DHCP Pool Config

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>lifetime</td>
<td>(Optional) Sets a length of time for the hosts to remember router advertisements. If configured, both valid and preferred lifetimes must be configured.</td>
</tr>
<tr>
<td>valid-lifetime</td>
<td>The amount of time, in seconds, the prefix remains valid for the requesting router to use. The range is from 60 through 4294967294. The preferred-lifetime value cannot exceed the valid-lifetime value.</td>
</tr>
<tr>
<td>preferred-lifetime</td>
<td>The amount of time, in seconds, that the prefix remains preferred for the requesting router to use. The range is from 60 through 4294967294. The preferred-lifetime value cannot exceed the valid-lifetime value.</td>
</tr>
<tr>
<td>infinite</td>
<td>An unlimited lifetime.</td>
</tr>
</tbody>
</table>
**Example:** The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool pool1:

```none
(Switch) #configure
(Switch) (Config)# ipv6 dhcp pool pool1
(Switch) (Config-dhcp6s-pool)# address prefix 2001::/64
(Switch) (Config-dhcp6s-pool)# exit
```

6.6.8 **domain-name (IPv6)**

This command sets the DNS domain name which is provided to DHCPv6 client by DHCPv6 server. DNS domain name is configured for stateless server support. Domain name consist of no more than 31 alpha-numeric characters. DHCPv6 pool can have multiple number of domain names with maximum of 8.

**Format**

```
domain-name dns-domain-name
```

**Mode**

IPv6 DHCP Pool Config

6.6.8.1 **no domain-name**

This command will remove dhcpv6 domain name from dhcpv6 pool.

**Format**

```
no domain-name dns-domain-name
```

**Mode**

IPv6 DHCP Pool Config

6.6.9 **dns-server (IPv6)**

This command sets the ipv6 DNS server address which is provided to dhcpv6 client by dhcpv6 server. DNS server address is configured for stateless server support. DHCPv6 pool can have multiple number of domain names with a maximum of 8.

**Format**

```
dns-server dns-server-address
```

**Mode**

IPv6 DHCP Pool Config

6.6.9.1 **no dns-server**

This command will remove DHCPv6 server address from DHCPv6 server.

**Format**

```
no dns-server dns-server-address
```

**Mode**

IPv6 DHCP Pool Config

6.6.10 **prefix-delegation (IPv6)**

Multiple IPv6 prefixes can be defined within a pool for distributing to specific DHCPv6 Prefix delegation clients. Prefix is the delegated IPv6 prefix. DUID is the client's unique DUID value (Example: 00:01:00:09:f8:79:4e:00:04:76:73:43:76'). Name is 31 characters textual client's name which is useful for logging or tracing only. Valid lifetime is the valid lifetime for the delegated prefix in seconds and preferred lifetime is the preferred lifetime for the delegated prefix in seconds.

**Default**

- valid-lifetime—2592000
- preferred-lifetime—604800

**Format**

```
prefix-delegation prefix/prefixlength DUID [name hostname][valid-lifetime 04294967295][preferred-lifetime 0-4294967295]
```

**Mode**

IPv6 DHCP Pool Config
6.6.10.1 no prefix-delegation
This command deletes a specific prefix-delegation client.

**Format**
no prefix-delegation prefix/prefix-delegation DUID

**Mode**
IPv6 DHCP Pool Config

6.6.11 show ipv6 dhcp
This command displays the DHCPv6 server name and status.

**Format**
show ipv6 dhcp

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 is Enabled</td>
<td>The status of the DHCPv6 server.</td>
</tr>
<tr>
<td>(Disabled)</td>
<td></td>
</tr>
<tr>
<td>Server DUID</td>
<td>If configured, shows the DHCPv6 unique identifier.</td>
</tr>
</tbody>
</table>

6.6.12 show ipv6 dhcp statistics
This command displays the IPv6 DHCP statistics for all interfaces.

**Format**
show ipv6 dhcp statistics

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Solicit Packets Received</td>
<td>Number of solicit received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Request Packets Received</td>
<td>Number of request received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Confirm Packets Received</td>
<td>Number of confirm received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Renew Packets Received</td>
<td>Number of renew received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Rebind Packets Received</td>
<td>Number of rebind received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Release Packets Received</td>
<td>Number of release received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Decline Packets Received</td>
<td>Number of decline received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Inform Packets Received</td>
<td>Number of inform received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Relay-forward Packets Received</td>
<td>Number of relay forward received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Relay-reply Packets Received</td>
<td>Number of relay-reply received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Malformed Packets Received</td>
<td>Number of malformed packets statistics.</td>
</tr>
<tr>
<td>Received DHCPv6 Packets Discarded</td>
<td>Number of DHCP discarded statistics.</td>
</tr>
<tr>
<td>Total DHCPv6 Packets Received</td>
<td>Total number of DHCPv6 received statistics.</td>
</tr>
<tr>
<td>DHCPv6 Advertisement Packets Transmitted</td>
<td>Number of advertise sent statistics.</td>
</tr>
<tr>
<td>DHCPv6 Reply Packets Transmitted</td>
<td>Number of reply sent statistics.</td>
</tr>
<tr>
<td>DHCPv6 Reconfig Packets Transmitted</td>
<td>Number of reconfigure sent statistics.</td>
</tr>
<tr>
<td>DHCPv6 Relay-reply Packets Transmitted</td>
<td>Number of relay-reply sent statistics.</td>
</tr>
<tr>
<td>DHCPv6 Relay-forward Packets Transmitted</td>
<td>Number of relay-forward sent statistics.</td>
</tr>
<tr>
<td>Total DHCPv6 Packets Transmitted</td>
<td>Total number of DHCPv6 sent statistics.</td>
</tr>
</tbody>
</table>
6.6.13 show ipv6 dhcp interface

This command displays DHCPv6 information for all relevant interfaces or the specified interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of a slot/port format. If you specify an interface, you can use the optional statistics parameter to view statistics for the specified interface.

**Format**

```
show ipv6 dhcp interface {slot/port|vlan 1-4093} [statistics]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Interface</td>
<td>The interface name in slot/port format.</td>
</tr>
<tr>
<td>Mode</td>
<td>Shows whether the interface is a IPv6 DHCP relay or server.</td>
</tr>
</tbody>
</table>

If the interface mode is server, the following information displays.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool Name</td>
<td>The pool name specifying information for DHCPv6 server distribution to DHCPv6 clients.</td>
</tr>
<tr>
<td>Server Preference</td>
<td>The preference of the server.</td>
</tr>
<tr>
<td>Option Flags</td>
<td>Shows whether rapid commit is enabled.</td>
</tr>
</tbody>
</table>

If the interface mode is relay, the following information displays.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Address</td>
<td>The IPv6 address of the relay server.</td>
</tr>
<tr>
<td>Relay Interface Number</td>
<td>The relay server interface in slot/port format.</td>
</tr>
<tr>
<td>Relay Remote ID</td>
<td>If configured, shows the name of the relay remote.</td>
</tr>
<tr>
<td>Option Flags</td>
<td>Shows whether rapid commit is configured.</td>
</tr>
</tbody>
</table>

If you use the statistics parameter, the command displays the IPv6 DHCP statistics for the specified interface. See “show ipv6 dhcp statistics” on page 718 for information about the output.

6.6.14 show ipv6 dhcp binding

This command displays configured DHCP pool.

**Format**

```
show ipv6 dhcp binding [ipv6-address]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Client Address</td>
<td>Address of DHCP Client.</td>
</tr>
<tr>
<td>DUID</td>
<td>String that represents the Client DUID.</td>
</tr>
<tr>
<td>IAID</td>
<td>Identity Association ID.</td>
</tr>
<tr>
<td>Prefix/Prefix Length</td>
<td>IPv6 address and mask length for delegated prefix.</td>
</tr>
<tr>
<td>Prefix Type</td>
<td>IPv6 Prefix type (IAPD, IANA, or IATA).</td>
</tr>
<tr>
<td>Client Address</td>
<td>Address of DHCP Client.</td>
</tr>
<tr>
<td>Client Interface</td>
<td>IPv6 Address of DHCP Client.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Address of DNS server address.</td>
</tr>
</tbody>
</table>
6.6.15 show ipv6 dhcp pool

This command displays configured DHCP pool.

**Format**

```
show ipv6 dhcp pool pool-name
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Pool Name</td>
<td>Unique pool name configuration.</td>
</tr>
<tr>
<td>Client DUID</td>
<td>Client's DHCP unique identifier. DUID is generated using the combination of the local system burned-in MAC address and a timestamp value.</td>
</tr>
<tr>
<td>Host</td>
<td>Name of the client.</td>
</tr>
<tr>
<td>Prefix/Prefix Length</td>
<td>IPv6 address and mask length for delegated prefix.</td>
</tr>
<tr>
<td>Preferred Lifetime</td>
<td>Preferred lifetime in seconds for delegated prefix.</td>
</tr>
<tr>
<td>Valid Lifetime</td>
<td>Valid lifetime in seconds for delegated prefix.</td>
</tr>
<tr>
<td>DNS Server Address</td>
<td>Address of DNS server address.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>DNS domain name.</td>
</tr>
</tbody>
</table>

6.6.16 show network ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the network management interface.

**Format**

```
show network ipv6 dhcp statistics
```

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Advertisement PacketsReceived</td>
<td>The number of DHCPv6 Advertisement packets received on the network interface.</td>
</tr>
<tr>
<td>DHCPv6 Reply Packets Received</td>
<td>The number of DHCPv6 Reply packets received on the network interface.</td>
</tr>
<tr>
<td>Received DHCPv6 Advertisement PacketsDiscarded</td>
<td>The number of DHCPv6 Advertisement packets discarded on the network interface.</td>
</tr>
<tr>
<td>Received DHCPv6 Reply Packets Discarded</td>
<td>The number of DHCPv6 Reply packets discarded on the network interface.</td>
</tr>
<tr>
<td>DHCPv6 Malformed Packets Received</td>
<td>The number of DHCPv6 packets that are received malformed on the network interface.</td>
</tr>
<tr>
<td>Total DHCPv6 Packets Received</td>
<td>The total number of DHCPv6 packets received on the network interface.</td>
</tr>
<tr>
<td>DHCPv6 Solicit Packets Transmitted</td>
<td>The number of DHCPv6 Solicit packets transmitted on the network interface.</td>
</tr>
<tr>
<td>DHCPv6 Request Packets Transmitted</td>
<td>The number of DHCPv6 Request packets transmitted on the network interface.</td>
</tr>
<tr>
<td>DHCPv6 Renew Packets Transmitted</td>
<td>The number of DHCPv6 Renew packets transmitted on the network interface.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

```
(admin)#show network ipv6 dhcp statistics
DHCPv6 Client Statistics

DHCPv6 Advertisement Packets Received.................... 0
DHCPv6 Reply Packets Received.............................. 0
Received DHCPv6 Advertisement Packets Discarded........ 0
Received DHCPv6 Reply Packets Discarded.................. 0
DHCPv6 Malformed Packets Received.......................... 0
Total DHCPv6 Packets Received.............................. 0

DHCPv6 Solicit Packets Transmitted......................... 0
DHCPv6 Request Packets Transmitted........................ 0
DHCPv6 Renew Packets Transmitted........................... 0
DHCPv6 Rebind Packets Transmitted.......................... 0
DHCPv6 Release Packets Transmitted........................ 0
Total DHCPv6 Packets Transmitted............................ 0
```

6.6.17  `show serviceport ipv6 dhcp statistics`

This command displays the statistics of the DHCPv6 client running on the serviceport management interface.

Format  `show serviceport ipv6 dhcp statistics`

Mode  - Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Advertisement Packets Received</td>
<td>The number of DHCPv6 Advertisement packets received on the service port interface.</td>
</tr>
<tr>
<td>DHCPv6 Reply Packets Received</td>
<td>The number of DHCPv6 Reply packets received on the service port interface.</td>
</tr>
<tr>
<td>Received DHCPv6 Advertisement Packets Discarded</td>
<td>The number of DHCPv6 Advertisement packets discarded on the service port interface.</td>
</tr>
<tr>
<td>Received DHCPv6 Reply Packets Discarded</td>
<td>The number of DHCPv6 Reply packets discarded on the service port interface.</td>
</tr>
<tr>
<td>DHCPv6 Malformed Packets Received</td>
<td>The number of DHCPv6 packets that are received malformed on the service port interface.</td>
</tr>
<tr>
<td>Total DHCPv6 Packets Received</td>
<td>The total number of DHCPv6 packets received on the service port interface.</td>
</tr>
<tr>
<td>DHCPv6 Solicit Packets Transmitted</td>
<td>The number of DHCPv6 Solicit packets transmitted on the service port interface.</td>
</tr>
<tr>
<td>DHCPv6 Request Packets Transmitted</td>
<td>The number of DHCPv6 Request packets transmitted on the service port interface.</td>
</tr>
<tr>
<td>DHCPv6 Renew Packets Transmitted</td>
<td>The number of DHCPv6 Renew packets transmitted on the service port interface.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

```
(Admin)#show serviceport ipv6 dhcp statistics
DHCPv6 Client Statistics

DHCPv6 Advertisement Packets Received.................... 0
DHCPv6 Reply Packets Received................................. 0
Received DHCPv6 Advertisement Packets Discarded............ 0
Received DHCPv6 Reply Packets Discarded.................... 0
DHCPv6 Malformed Packets Received............................. 0
Total DHCPv6 Packets Received................................. 0

DHCPv6 Solicit Packets Transmitted............................ 0
DHCPv6 Request Packets Transmitted............................. 0
DHCPv6 Renew Packets Transmitted............................... 0
DHCPv6 Rebind Packets Transmitted.............................. 0
DHCPv6 Release Packets Transmitted............................. 0
Total DHCPv6 Packets Transmitted............................... 0
```

6.6.18 clear ipv6 dhcp

Use this command to clear DHCPv6 statistics for all interfaces or for a specific interface. Use the `slot/port` parameter to specify the interface.

```
Format       clear ipv6 dhcp {statistics | interface slot/port statistics}
Mode         Privileged EXEC
```

6.6.19 clear ipv6 dhcp binding

This command deletes an automatic address binding from the DHCP server database. `address` is a valid IPv6 address. A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator runs the `clear ipv6 dhcp binding` command.

If the `clear ipv6 dhcp binding` command is used with the optional `ipv6-address` argument specified, only the binding for the specified client is deleted. If the `clear ipv6 dhcp binding` command is used without the `ipv6-address` argument, all automatic client bindings are deleted from the DHCP for IPv6 binding table.

```
Format       clear ipv6 dhcp binding [ipv6-address]
Mode         Privileged EXEC
```

6.6.20 clear network ipv6 dhcp statistics

Use this command to clear the DHCPv6 statistics on the network management interface.

```
Format       clear network ipv6 dhcp statistics
Mode         Privileged EXEC
```
6.6.21 clear serviceport ipv6 dhcp statistics
Use this command to clear the DHCPv6 client statistics on the service port interface.

Format: clear serviceport ipv6 dhcp statistics
Mode: Privileged EXEC

6.7 DHCPv6 Snooping Configuration Commands
This section describes commands you use to configure IPv6 DHCP Snooping.

6.7.1 ipv6 dhcp snooping
Use this command to globally enable IPv6 DHCP Snooping.

Default: disabled
Format: ipv6 dhcp snooping
Mode: Global Config

6.7.1.1 no ipv6 dhcp snooping
Use this command to globally disable IPv6 DHCP Snooping.

Format: no ipv6 dhcp snooping
Mode: Global Config

6.7.2 ipv6 dhcp snooping vlan
Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default: disabled
Format: ipv6 dhcp snooping vlan vlan-list
Mode: Global Config

6.7.2.1 no ipv6 dhcp snooping vlan
Use this command to disable DHCP Snooping on VLANs.

Format: no ipv6 dhcp snooping vlan vlan-list
Mode: Global Config

6.7.3 ipv6 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: ipv6 dhcp snooping verify mac-address
Mode: Global Config
6.7.3.1 no ipv6 dhcp snooping verify mac-address
Use this command to disable verification of the source MAC address with the client hardware address.

**Format**
```
no ipv6 dhcp snooping verify mac-address
```

**Mode**
Global Config

6.7.4 ipv6 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**
```
ipv6 dhcp snooping database {local|tftp://hostIP/filename}
```

**Mode**
Global Config

6.7.5 ip dhcp snooping database write-delay
Use this command to configure the interval in seconds at which the DHCP Snooping database is 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

6.7.5.1 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

6.7.6 ipv6 dhcp snooping binding
Use this command to configure static DHCP Snooping binding.

**Format**
```
ipv6 dhcp snooping binding mac-address vlan vlan-id ip address interface interface-id
```

**Mode**
Global Config

6.7.6.1 no ipv6 dhcp snooping binding
Use this command to remove the DHCP static entry from the DHCP Snooping database.

**Format**
```
no ipv6 dhcp snooping binding mac-address
```

**Mode**
Global Config
6.7.7  ipv6 dhcp snooping trust
Use this command to configure an interface or range of interfaces as trusted.

Default: disabled
Format: ipv6 dhcp snooping trust
Mode: Interface Config

6.7.7.1  no ipv6 dhcp snooping trust
Use this command to configure the port as untrusted.

Format: no ipv6 dhcp snooping trust
Mode: Interface Config

6.7.8  ipv6 dhcp snooping log-invalid
Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default: disabled
Format: ipv6 dhcp snooping log-invalid
Mode: Interface Config

6.7.8.1  no ipv6 dhcp snooping log-invalid
Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format: no ipv6 dhcp snooping log-invalid
Mode: Interface Config

6.7.9  ipv6 dhcp snooping limit
Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second. The burst level range is 1 to 15 seconds. Rate limiting is configured on a physical port and may be applied to trusted and untrusted ports.

Default: disabled (no limit)
Format: ipv6 dhcp snooping limit {rate pps [burst interval seconds]}
Mode: Interface Config
### 6.7.9.1 no ipv6 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**
```
nop ipv6 dhcp snooping limit
```

**Mode**
Interface Config

### 6.7.10 ipv6 verify source

Use this command to configure the IPv6SG 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 is filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

**Default**
the source ID is the IP address

**Format**
```
ipv6 verify source {port-security}
```

**Mode**
Interface Config

#### 6.7.10.1 no ipv6 verify source

Use this command to disable the IPv6SG configuration in the hardware. You cannot disable port-security alone if it is configured.

**Format**
```
no ipv6 verify source
```

**Mode**
Interface Config

### 6.7.11 ipv6 verify binding

Use this command to configure static IPv6 source guard (IPv6SG) entries.

**Format**
```
ipv6 verify binding mac-address vlan id ipv6 address interface interface id
```

**Mode**
Global Config

#### 6.7.11.1 no ipv6 verify binding

Use this command to remove the IPv6SG static entry from the IPv6SG database.

**Format**
```
no ipv6 verify binding mac-address vlan id ipv6 address interface interface id
```

**Mode**
Global Config

### 6.7.12 show ipv6 dhcp snooping

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

**Format**
```
show ipv6 dhcp snooping
```

**Mode**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface for which data is displayed.</td>
</tr>
<tr>
<td>Trusted</td>
<td>If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.</td>
</tr>
<tr>
<td>Log Invalid Pkts</td>
<td>If it is enabled, DHCP snooping application logs invalid packets on the specified interface.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(switch) #show ipv6 dhcp snooping

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Log</th>
<th>Invalid Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>0/2</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>0/3</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>0/4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>0/6</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

6.7.13 show ipv6 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 ipv6 dhcp snooping binding [{static/dynamic}] [interface slot/port] [vlan id]

Mode:
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Displays the valid IPv6 address for the binding rule.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN for the binding rule.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface to add a binding into the DHCP snooping interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Binding type; statically configured from the CLI or dynamically learned.</td>
</tr>
<tr>
<td>Lease (sec)</td>
<td>The remaining lease time for the entry.</td>
</tr>
</tbody>
</table>

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

(switch) #show ipv6 dhcp snooping binding

Total number of bindings: 2

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IPv6 Address</th>
<th>VLAN</th>
<th>Interface</th>
<th>Type</th>
<th>Lease time (Secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:B3:06:60:80</td>
<td>2000::1/64</td>
<td>10</td>
<td>0/1</td>
<td></td>
<td>86400</td>
</tr>
<tr>
<td>00:0F:FE:00:13:04</td>
<td>3000::1/64</td>
<td>10</td>
<td>0/1</td>
<td></td>
<td>86400</td>
</tr>
</tbody>
</table>
6.7.14  show ipv6 dhcp snooping database

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

**Format**  
show ipv6 dhcp snooping database

**Mode**  
- Privileged EXEC
- User EXEC

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent URL</td>
<td>Bindings database agent URL.</td>
</tr>
<tr>
<td>Write Delay</td>
<td>The maximum write time to write the database into local or remote.</td>
</tr>
</tbody>
</table>

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

(switch) #show ipv6 dhcp snooping database

agent url: /10.131.13.79:/sain.txt
write-delay: 5000

6.7.15  show ipv6 dhcp snooping interfaces

Use this command to show the DHCP Snooping status of all interfaces or a specified interface.

**Format**  
show ipv6 dhcp snooping interfaces [interface slot/port]

**Mode**  
Privileged EXEC

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

(switch) #show ipv6 dhcp snooping interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate Limit (pps)</th>
<th>Burst Interval (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/g1</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1/g2</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>1/g3</td>
<td>No</td>
<td>15</td>
<td>1</td>
</tr>
</tbody>
</table>

(switch) #show ip dhcp snooping interfaces ethernet 0/1

<table>
<thead>
<tr>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
</tr>
<tr>
<td>Trust State</td>
</tr>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

6.7.16  show ipv6 dhcp snooping statistics

Use this command to list statistics for IPv6 DHCP Snooping security violations on untrusted ports.

**Format**  
show ipv6 dhcp snooping statistics

**Mode**  
- Privileged EXEC
- User EXEC
Example: The following shows example CLI display output for the command.

(switch) #show ipv6 dhcp snooping statistics

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Verify Failures</th>
<th>Client Ifc Mismatch</th>
<th>DHCP Server Msgs Rec’d</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/13</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/14</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/15</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/16</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/17</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/18</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/19</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/20</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

6.7.17 clear ipv6 dhcp snooping binding

Use this command to clear all DHCPv6 Snooping bindings on all interfaces or on a specific interface.

Format: clear ipv6 dhcp snooping binding [interface slot/port]

Mode
- Privileged EXEC
- User EXEC

6.7.18 clear ipv6 dhcp snooping statistics

Use this command to clear all DHCPv6 Snooping statistics.

Format: clear ipv6 dhcp snooping statistics

Mode
- Privileged EXEC
- User EXEC
6.7.19 show ipv6 verify

Use this command to display the IPv6 configuration on a specified slot/port.

**Format**

```
show ipv6 verify interface
```

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface address in slot/port format.</td>
</tr>
<tr>
<td>Filter Type</td>
<td>Is one of two values:</td>
</tr>
<tr>
<td></td>
<td>• ip-v6mac: User has configured MAC address filtering on this interface.</td>
</tr>
<tr>
<td></td>
<td>• ipv6: Only IPv6 address filtering on this interface.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>IPv6 address of the interface</td>
</tr>
<tr>
<td>MAC Address</td>
<td>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.”</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN for the binding rule.</td>
</tr>
</tbody>
</table>

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

```
(switch) #show ipv6 verify 0/1
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter Type</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>ipv6-mac</td>
<td>2000::1/64</td>
<td>00:02:B3:06:60:80</td>
<td>10</td>
</tr>
<tr>
<td>0/1</td>
<td>ipv6-mac</td>
<td>3000::1/64</td>
<td>00:0F:FE:00:13:04</td>
<td>10</td>
</tr>
</tbody>
</table>

6.7.20 show ipv6 verify source

Use this command to display the IPv6SG configurations on all ports. If the interface option is specified, the output is restricted to the specified slot/port.

**Format**

```
show ipv6 verify source [interface]
```

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface address in slot/port format.</td>
</tr>
<tr>
<td>Filter Type</td>
<td>Is one of two values:</td>
</tr>
<tr>
<td></td>
<td>• ip-v6mac: User has configured MAC address filtering on this interface.</td>
</tr>
<tr>
<td></td>
<td>• ipv6: Only IPv6 address filtering on this interface.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>IPv6 address of the interface</td>
</tr>
<tr>
<td>MAC Address</td>
<td>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.”</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN for the binding rule.</td>
</tr>
</tbody>
</table>

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

```
(switch) #show ipv6 verify source
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter Type</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>ipv6-mac</td>
<td>2000::1/64</td>
<td>00:02:B3:06:60:80</td>
<td>10</td>
</tr>
<tr>
<td>0/1</td>
<td>ipv6-mac</td>
<td>3000::1/64</td>
<td>00:0F:FE:00:13:04</td>
<td>10</td>
</tr>
</tbody>
</table>
6.7.21 show ipv6 source binding

Use this command to display the IPv6SG bindings.

**Format**

```
show ipv6 source binding [{dhcp-snooping|static}] [interface slot/port] [vlan id]
```

**Mode**

- Privileged EXEC
- User EXEC

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

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

```
(switch) #show ipv6 source binding
```

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Type</th>
<th>Vlan</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:08</td>
<td>2000::1</td>
<td>dhcp-snooping</td>
<td>2</td>
<td>0/1</td>
</tr>
<tr>
<td>00:00:00:00:00:09</td>
<td>3000::1</td>
<td>dhcp-snooping</td>
<td>3</td>
<td>0/1</td>
</tr>
<tr>
<td>00:00:00:00:00:0A</td>
<td>4000::1</td>
<td>dhcp-snooping</td>
<td>4</td>
<td>0/1</td>
</tr>
</tbody>
</table>
7/ Quality of Service Commands

This chapter describes the Quality of Service (QoS) commands available in the FASTPATH CLI.

The QoS Commands chapter contains the following sections:

- “Class of Service Commands” on page 732
- “Differentiated Services Commands” on page 742
- “DiffServ Class Commands” on page 743
- “DiffServ Policy Commands” on page 750
- “DiffServ Service Commands” on page 756
- “DiffServ Show Commands” on page 757
- “MAC Access Control List Commands” on page 762
- “IP Access Control List Commands” on page 769
- “IPV6 Access Control List Commands” on page 784
- “Time Range Commands for Time-Based ACLs” on page 792
- “Auto-Voice over IP Commands” on page 794
- “iSCSI Optimization Commands” on page 798

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.

7.1 Class of Service Commands

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

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

7.1.1 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.

**Format**

```
classofservice dot1p-mapping userpriority trafficclass
```

**Modes**

- Global Config
- Interface Config
7.1.1  no classofservice dot1p-mapping
This command maps each 802.1p priority to its default internal traffic class value.

**Format**
```plaintext
no classofservice dot1p-mapping
```

**Modes**
- Global Config
- Interface Config

7.1.2  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**
```plaintext
classofservice ip-dscp-mapping ipdscp trafficclass
```

**Mode**
- Global Config

7.1.2.1  no classofservice ip-dscp-mapping
This command maps each IP DSCP value to its default internal traffic class value.

**Format**
```plaintext
no classofservice ip-dscp-mapping
```

**Mode**
- Global Config

7.1.3  classofservice ip-precedence-mapping
This command maps an IP Precedence value to an internal traffic class for a specific interface. The 0-7 parameter is optional and is only valid on platforms that support independent per-port class of service mappings.

**Format**
```plaintext
classofservice ip-precedence-mapping 0-7
```

**Mode**
- Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>The IP Precedence value.</td>
</tr>
</tbody>
</table>
7.1.3.1 no classofservice ip-precedence-mapping
This command returns the mapping to its default value.

Format: no classofservice ip-dscp-mapping
Mode: Global Config

7.1.4 classofservice trust
This command sets the class of service trust mode of an interface or range of interfaces. 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.

Format:
no classofservice trust
Mode: Global Config

**Notice**
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 | untrusted}
Modes:
- Global Config
- Interface Config

7.1.4.1 no classofservice trust
This command sets the interface mode to the default value.

Format: no classofservice trust
Modes:
- Global Config
- Interface Config

7.1.5 cos-queue max-bandwidth
This command specifies the maximum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. 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 maximum bandwidth. The sum of all values entered must not exceed 100.

Format: cos-queue max-bandwidth bw-0 bw-1 ... bw-n
Modes:
- Global Config
- Interface Config
7.1.5.1  no cos-queue max-bandwidth
This command restores the default for each queue’s minimum bandwidth value.

**Format**  
no cos-queue min-bandwidth

**Modes**  
- Global Config
- Interface Config

7.1.6  cos-queue min-bandwidth
This command specifies the minimum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. 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

7.1.6.1  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

7.1.7  cos-queue random-detect
This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the `random-detect queue-parms` and `random-detect exponential-weighting-constant` commands.

**Format**  
cos-queue random-detect queue-id-1 [queue-id-2 ... queue-id-n]

**Modes**  
- Global Config
- Interface Config

When specified in Interface Config’ mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

At least one, but no more than n queue-id values are specified with this command. Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (n−1), where n is the total number of queues supported per interface. The number n = 7 and corresponds to the number of supported queues (traffic classes).
7.1.7.1 no cos-queue random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Format
\[
\text{no cos-queue random-detect queue-id-1 [queue-id-2 ... queue-id-n]}
\]

Modes
- Global Config
- Interface Config

7.1.8 cos-queue strict

This command activates the strict priority scheduler mode for each specified queue for an interface queue on an interface, a range of interfaces, or all interfaces.

Format
\[
\text{cos-queue strict queue-id-1 [queue-id-2 ... queue-id-n]}
\]

Modes
- Global Config
- Interface Config

7.1.8.1 no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format
\[
\text{no cos-queue strict queue-id-1 [queue-id-2 ... queue-id-n]}
\]

Modes
- Global Config
- Interface Config

7.1.9 random-detect

This command is used to enable WRED for the interface as a whole, and is only available when per-queue WRED activation control is not supported by the device. Specific WRED parameters are configured using the random-detect queue-parms and the random-detect exponential-weighting-constant commands.

Format
\[
\text{random-detect}
\]

Modes
- Global Config
- Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.
7.1.9.1 no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

**Format**

no random-detect

**Modes**

- Global Config
- Interface Config

7.1.10 random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

**Format**

random-detect exponential-weighting-constant 0-15

**Modes**

- Global Config
- Interface Config

7.1.10.1 no random-detect exponential-weighting-constant

Use this command to set the WRED decay exponent back to the default.

**Format**

no random-detect exponential-weighting-constant

**Modes**

- Global Config
- Interface Config

7.1.11 random-detect queue-parms

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the cos-queue random-detect command).

**Format**

random-detect queue-parms queue-id-1 [queue-id-2 ... queue-id-n] min-thresh thresh-prec-1 ... thresh-prec-n max-thresh thresh-prec-1 ... thresh-prec-n drop-probability prob-prec-1 ... prob-prec-n

**Modes**

- Global Config
- Interface Config

Each parameter is specified for each possible drop precedence (color of TCP traffic). The last precedence applies to all non-TCP traffic. For example, in a 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>min-thresh</td>
<td>The minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.</td>
</tr>
<tr>
<td>max-thresh</td>
<td>The maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.</td>
</tr>
<tr>
<td>drop-probability</td>
<td>The percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).</td>
</tr>
</tbody>
</table>
7.1.11  no random-detect queue-parms
Use this command to set the WRED configuration back to the default.

Format  no random-detect queue-parms queue-id-1 [queue-id-2 ... queue-id-n]
Modes  •  Global Config
       •  Interface Config

7.1.12  traffic-shape
This command specifies the maximum transmission bandwidth limit for the interface as a whole. The bandwidth values are from 0-100 in increments of 1. You can also specify this value for a range of interfaces or all interfaces. 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

7.1.12.1  no traffic-shape
This command restores the interface shaping rate to the default value.

Format  no traffic-shape
Modes  •  Global Config
       •  Interface Config

7.1.13  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 "Voice VLAN Commands" on page 344.

Format  show classofservice dot1p-mapping [slot/port]
Mode  Privileged EXEC

The following information is repeated for each user priority.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Priority</td>
<td>The 802.1p user priority value.</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>The traffic class internal queue identifier to which the user priority value is mapped.</td>
</tr>
</tbody>
</table>

7.1.14  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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP DSCP</td>
<td>The IP DSCP value.</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>The traffic class internal queue identifier to which the IP DSCP value is mapped.</td>
</tr>
</tbody>
</table>

### 7.1.15 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Precedence</td>
<td>The IP Precedence value.</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>The traffic class internal queue identifier to which the IP Precedence value is mapped.</td>
</tr>
</tbody>
</table>

### 7.1.16 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of Service Trust Mode</td>
<td>The trust mode, which is either Dot1P, IP DSCP, or Untrusted.</td>
</tr>
<tr>
<td>Non-IP Traffic Class</td>
<td>(IP DSCP mode only) The traffic class used for non-IP traffic.</td>
</tr>
<tr>
<td>Untrusted Traffic Class</td>
<td>(Untrusted mode only) The traffic class used for all untrusted traffic.</td>
</tr>
</tbody>
</table>

### 7.1.17 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Shaping Rate</td>
<td>The global interface shaping rate value.</td>
</tr>
<tr>
<td>WRED Decay Exponent</td>
<td>The global WRED decay exponent value.</td>
</tr>
<tr>
<td>Queue Id</td>
<td>An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.</td>
</tr>
</tbody>
</table>
If you specify the interface, the command also displays the following information.

### Minimum Bandwidth
The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.

### Maximum Bandwidth
The maximum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.

### Scheduler Type
Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.

### Queue Management Type
The queue depth management technique used for this queue (tail drop).

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface ID</td>
<td>The slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.</td>
</tr>
<tr>
<td>Interface Shaping Rate</td>
<td>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.</td>
</tr>
<tr>
<td>WRED Decay Exponent</td>
<td>The configured WRED decay exponent for a CoS queue interface.</td>
</tr>
</tbody>
</table>

#### 7.1.18 show interfaces random-detect
This command displays the global WRED settings for each CoS queue. If you specify the slot/port, the command displays the WRED settings for each CoS queue on the specified interface.

**Format**
```
show interfaces random-detect [slot/port]
```

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue ID</td>
<td>An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.</td>
</tr>
<tr>
<td>WRED Minimum Threshold</td>
<td>The configured minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.</td>
</tr>
<tr>
<td>WRED Maximum Threshold</td>
<td>The configured maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.</td>
</tr>
<tr>
<td>WRED Drop Probability</td>
<td>The configured percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).</td>
</tr>
</tbody>
</table>

#### 7.1.19 show interfaces tail-drop-threshold
This command displays the tail drop threshold information. If you specify the slot/port, the command displays the tail drop threshold information for the specified interface.

**Format**
```
show interfaces tail-drop-threshold [slot/port]
```

**Mode**
Privileged EXEC
7.1.20 show protection-group

This command lists the protection groups. All or specified protection groups 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

Mode Privileged EXEC

7.1.21 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.

For stacking this command is only valid inside a unit (receiving and sending ports in same unit).

Format

protection-group <0..3>
protection-group <0..3> name name

Mode Global Config

7.1.21.1 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

7.1.22 protection-group (interface)

This command includes/excludes interfaces to/from a protection group or sets an egress-mask for an interface.

If an interface is member in a protection group it may sent packets to interfaces which are not member of any group (unprotected) and to interfaces in the same group, but not to interfaces in another group. An egress-mask is calculated based on the protection-groups containing for each interface (bit 0 for first interface) a bit, indicating that it is allowed (1) or prohibited (0) to forward to this interface. The calculated egress-mask can be displayed by 'show protection-group mask' below.

The calculated egress-mask may be overridden by setting directly this mask (use parameter "mask"). This is not supported for stacking mode.

For a LAG the minimal egress mask over all member interfaces (either calculated for protection-groups or directly set) is used (<mask-member-1> & ... & <mask-member-N>).

Format

protection-group {<0..3> | mask <mask>}

Mode Interface Config
7.1.22.1 no protection-group (interface)
The command deletes an interface to a protection group or deletes an egress port mask. The command deletes an egress mask for an interface if specifying the keyword 'mask'.

Format: no protection-group {<0..3> / mask <mask>}
Mode: Interface Config

7.2 Differentiated Services Commands
This section describes the commands you use to configure QOS Differentiated Services (DiffServ).
You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
   a. Creating and deleting classes.
   b. Defining match criteria for a class.

2. Policy
   a. Creating and deleting policies
   b. Associating classes with a policy
   c. Defining policy statements for a policy/class combination

3. Service
   a. Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:
- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

---

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.

---

7.2.1 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
7.2.1.1  

**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

7.3  

**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.

---

**NOTICE**

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`.

7.3.1  

**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.

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.

---

**NOTICE**

The class-map-name ‘default’ is reserved and must not be used.

---

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.

The optional keyword `appiq` creates a new DiffServ appiq class. Regular expressions found in the traffic patterns in layer 7 applications can be matched to the App-IQ class using a `match signature` command.

---

**NOTICE**

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 [appiq | ipv4 | ipv6]`

**Mode**

Global Config
7.3.1 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

7.3.2 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

7.3.3 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, mplsmcast, netbios, novell, pppoe, rarp or as a custom EtherType value in the range of 0x0600-0xFFFF. Use the [not] option to negate the match condition.

This command is not available on the Broadcom BCM5630x platform.

Format match [not] ethertype {keyword | custom 0x0600-0xFFFF}
Mode Class-Map Config
Ipv6-Class-Map Config

7.3.4 match any
This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. Use the [not] option to negate the match condition.

Default none
Format match [not] any
Mode Class-Map Config
Ipv6-Class-Map Config

7.3.5 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
7.3.5.1 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

7.3.6 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. Use the `[not]` option to negate the match condition.

Format
```
match [not] cos 0-7
```

Mode
- Class-Map Config
- Ipv6-Class-Map Config

7.3.7 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. Use the `[not]` option to negate the match condition.

This command is supported on the following platforms:
- BCM56314
- BCM56504
- BCM56214
- BCM56224

Notice
- The parameters `refclassname` and `class-map-name` can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the `refclassname` class while the class is still referenced by any `class-map-name` fails.
- The combined match criteria of `class-map-name` and `refclassname` must be an allowed combination based on the class type.
- Any subsequent changes to the `refclassname` class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.
7.3.8 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). Use the `[not]` option to negate the match condition.

Default: none
Format: `match [not]destination-address mac macaddr macmask`
Mode: Class-Map Config
Ipv6-Class-Map Config

7.3.9 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. Use the `[not]` option to negate the match condition.

Default: none
Format: `match [not] dstip ipaddr ipmask`
Mode: Class-Map Config

7.3.10 match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet. Use the `[not]` option to negate the match condition.

Default: none
Format: `match [not] dstip6 destination-ipv6-prefix/prefix-length`
Mode: Ipv6-Class-Map Config

7.3.11 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. Use the `[not]` option to negate the match condition.
7.3.12 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. Use the `[not]` option to negate the match condition.

**Default** none

**Format**

`match [not] dst14port {portkey | 0-65535}`

**Mode**

Class-Map Config
Ipv6-Class-Map Config

7.3.13 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. Use the `[not]` option to negate the match condition.

**Default** none

**Format**

`match [not] ip dscp dscpval`

**Mode**

Class-Map Config
Ipv6-Class-Map Config

7.3.14 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). Use the `[not]` option to negate the match condition.

**Default** none

**Format**

`match [not] ip precedence 0-7`

**Mode**

Class-Map Config

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.
7.3.15 match ip6flowlbl

Use this command to enter an IPv6 flow label value. Use the [not] option to negate the match condition.

Default: none

Format: match [not] ip6flowlbl label 0-1048575

Mode: IPv6-Class-Map Config

7.3.16 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. Use the [not] option to negate the match condition.

Default: none

Format: match [not] protocol {protocol-name | 0-255}

Mode: Class-Map Config

7.3.17 match signature

This command maps the available signatures from the rules file to the AppIQ class. When the appiq class is created, this menu displays an index number and its signature pattern. A single signature can be mapped using a number or multiple signatures can be selected and mapped to a class. Using this command without an index value maps all the available signatures to the same class.

Default: none

Format: match signature [<StartIndex>-<EndIndex>]

Mode: Class-Map Config

7.3.18 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). Use the [not] option to
negate the match condition.

### 7.3.19 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. Use the `[not]` option to negate the match condition.

**Default**: none  
**Format**: `match [not] source-address mac address macmask`  
**Mode**: Class-Map Config, Ipv6-Class-Map Config

### 7.3.20 match srcip6
This command adds to the specified class definition a match condition based on the source IP address of a packet. Use the `[not]` option to negate the match condition.

**Default**: none  
**Format**: `match [not] srcip ipv6-prefix/prefix-length`  
**Mode**: Class-Map Config

### 7.3.21 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. Use the `[not]` option to negate the match condition.

**Default**: none  
**Format**: `match [not] srcip6 source-ipv6-prefix/prefix-length`  
**Mode**: Class-Map Config, Ipv6-Class-Map Config

### 7.3.22 match src port
This command adds a match condition for a range of layer source 4 ports. If an interface receives traffic that is within the configured range of layer 4 source ports, then only the appiq class is in effect. `portvalue` specifies a single source port.

**Default**: none  
**Format**: `match src port {portstart-portend | portvalue}`  
**Mode**: Class-Map Config
7.3.23 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 0 to 4093. Use the [not] option to negate the match condition.

**NOTICE**

This command is not available on the Broadcom 5630x platform.

<table>
<thead>
<tr>
<th>Default</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>match [not] vlan 0-4093</td>
</tr>
<tr>
<td>Mode</td>
<td>Class-Map Config</td>
</tr>
<tr>
<td></td>
<td>Ipv6-Class-Map Config</td>
</tr>
</tbody>
</table>

7.3.24 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 0 to 4093. Use the [not] option to negate the match condition.

**NOTICE**

This command is not available on the Broadcom 5630x platform.

<table>
<thead>
<tr>
<th>Default</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>match [not] secondary-vlan 0-4093</td>
</tr>
<tr>
<td>Mode</td>
<td>Class-Map Config</td>
</tr>
<tr>
<td></td>
<td>Ipv6-Class-Map Config</td>
</tr>
</tbody>
</table>

7.4 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.

**NOTICE**

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`.

7.4.1 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.

<table>
<thead>
<tr>
<th>Format</th>
<th>assign-queue <code>queueid</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Policy-Class-Map Config</td>
</tr>
<tr>
<td>Incompatibilities</td>
<td>Drop</td>
</tr>
</tbody>
</table>
7.4.2 drop
This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format: drop
Mode: Policy-Class-Map Config
Incompatibilities: Assign Queue, Mark (all forms), Mirror, Police, Redirect

7.4.3 mirror
This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Format: mirror slot/port
Mode: Policy-Class-Map Config
Incompatibilities: Drop, Redirect

7.4.4 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).

Format: redirect slot/port
Mode: Policy-Class-Map Config
Incompatibilities: Drop, Mirror

7.4.5 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.

Format: conform-color class-map-name
Mode: Policy-Class-Map Config

This command may only be used after specifying a police command for the policy-class instance.
7.4.6 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.

This command causes the specified policy to create a reference to the class definition.

**NOTICE**

The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

**Format**

```
class classname
```

**Mode**

Policy-Map Config

7.4.6.1 no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. `classname` is the name of an existing DiffServ class.

This command removes the reference to the class definition for the specified policy.

**Format**

```
no class classname
```

**Mode**

Policy-Map Config

7.4.7 mark cos

This command marks all packets for the associated traffic stream with the specified class of service (CoS) value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

**Default**

1

**Format**

```
mark-cos 0-7
```

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Mark IP DSCP, IP Precedence, Police

7.4.8 mark secondary-cos

This command marks the outer VLAN tags in the packets for the associated traffic stream as secondary CoS.

**Default**

1

**Format**

```
mark secondary-cos 0-7
```

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Mark IP DSCP, IP Precedence, Police
7.4.9  mark cos-as-sec-cos
This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking Cos as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format     mark-cos-as-sec-cos
Mode       Policy-Class-Map Config
Incompatibilities  Drop, Mark IP DSCP, IP Precedence, Police

Example: The following shows an example of the command.
(switch) (Config-policy-classmap)#mark cos-as-sec-cos

7.4.10  mark ip-dscp
This command marks all packets for the associated traffic stream with the specified IP DSCP value.
The dscpval value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, 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

7.4.11  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.

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

7.4.12  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-as-sec-cos, set-cos-transmit, set-sec-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. These actions can be set with this command once the style has been configured.

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.
These actions can be set with this command once the style has been configured.

**Example:** The following shows an example of the command.

```plaintext
(switch) (Config-policy-classmap)#policy-simple 1 128 conform-action transmit violate-action drop
```

### 7.4.13 policy-single-rate

This command is the single-rate form of the policy command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cost, set-cos-transmit, set-sec-cos-transmit, set-prec-transmit, or transmit. In this single-rate form of the policy command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

**Format**

```
```

**Mode**

Policy-Class-Map Config

### 7.4.14 policy-two-rate

This command is the two-rate form of the policy command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cost, set-cos-transmit, set-sec-cos-transmit, set-prec-transmit, or transmit. In this two-rate form of the policy command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

**Format**

```
```

**Mode**

Policy-Class-Map Config

### 7.4.15 policy-map

This command establishes a new DiffServ policy. The **policy-name** 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, or the outbound traffic direction as indicated by the `out` parameter, respectively.

---

**Notice:**

The CLI mode is changed to Policy-Map Config when this command is successfully executed.
7.4.15.1 no policy-map
This command eliminates an existing DiffServ policy. The `policyname` parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format: `no policy-map policyname`
Mode: Global Config

7.4.16 policy-map rename
This command changes the name of a DiffServ policy. The `policyname` is the name of an existing DiffServ class. The `newpolicyname` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format: `policy-map rename policyname newpolicyname`
Mode: Global Config

7.4.17 show protection-group
This command lists the protection groups. All or specified protection groups 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`
Mode: Privileged EXEC

7.4.18 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.

For stacking this command is only valid inside a unit (receiving and sending ports in same unit).

Format: `protection-group <0..3>`
         `protection-group <0..3> name name`
Mode: Global Config
7.4.18.1 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

7.4.19 protection-group (interface)

This command includes/excludes interfaces to/from a protection group or sets an egress-mask for an interface.

If an interface is member in a protection group it may sent packets to interfaces which are not member of any group (unprotected) and to interfaces in the same group, but not to interfaces in another group. An egress-mask is calculated based on the protection-groups containing for each interface (bit 0 for first interface) a bit, indicating that it is allowed (1) or prohibited (0) to forward to this interface. The calculated egress-mask can be displayed by "show protection-group mask" below.

The calculated egress-mask may be overridden by setting directly this mask (use parameter "mask"). This is not supported for stacking mode.

For a LAG the minimal egress mask over all member interfaces (either calculated for protection-groups or directly set) is used (<mask-member-1> & … & <mask-member-N>).

Format

protection-group {<0..3> | mask <mask>}

Mode

Interface Config

7.4.19.1 no protection-group (interface)

The command deletes an interface to a protection group or deletes an egress port mask. The command deletes an egress mask for an interface if specifying the keyword 'mask'.

Format

no protection-group {<0..3> | mask <mask>}

Mode

Interface Config

7.5 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.

7.5.1 service-policy

This command attaches a policy to an interface in the inbound direction as indicated by the in parameter, or the outbound direction as indicated by the out parameter, respectively. The policyname parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.
7.5.1.1 no service-policy

This command detaches a policy from an interface in the inbound direction as indicated by the `in` parameter, or the outbound direction as indicated by the `out` parameter, respectively. The `policyname` parameter is the name of an existing DiffServ policy.

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.

Each interface can have one policy attached.

7.6 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.

7.6.1 show class-map

This command displays all configuration information for the specified class. The `class-name` is the name of an existing DiffServ class.

If the class-name is specified the following fields are displayed:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Name</td>
<td>The name of this class.</td>
</tr>
<tr>
<td>Class Type</td>
<td>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.</td>
</tr>
<tr>
<td>Class Layer3 Protocol</td>
<td>The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.</td>
</tr>
</tbody>
</table>
If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Name</td>
<td>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.)</td>
</tr>
<tr>
<td>Class Type</td>
<td>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.</td>
</tr>
<tr>
<td>Ref Class Name</td>
<td>The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.</td>
</tr>
</tbody>
</table>

7.6.2 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiffServ Admin mode</td>
<td>The current value of the DiffServ administrative mode.</td>
</tr>
<tr>
<td>Class Table Size Current/Max</td>
<td>The current and maximum number of entries (rows) in the Class Table.</td>
</tr>
<tr>
<td>Class Rule Table Size Current/Max</td>
<td>The current and maximum number of entries (rows) in the Class Rule Table.</td>
</tr>
<tr>
<td>Policy Table Size Current/Max</td>
<td>The current and maximum number of entries (rows) in the Policy Table.</td>
</tr>
<tr>
<td>Policy Instance Table Size Current/Max</td>
<td>The current and maximum number of entries (rows) in the Policy Instance Table.</td>
</tr>
<tr>
<td>Policy Instance Table Max Current/Max</td>
<td>The current and maximum number of entries (rows) for the Policy Instance Table.</td>
</tr>
<tr>
<td>Policy Attribute Table Max Current/Max</td>
<td>The current and maximum number of entries (rows) for the Policy Attribute Table.</td>
</tr>
<tr>
<td>Service Table Size Current/Max</td>
<td>The current and maximum number of entries (rows) in the Service Table.</td>
</tr>
</tbody>
</table>

7.6.3 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:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>The name of this policy.</td>
</tr>
<tr>
<td>Policy Type</td>
<td>The policy type (only inbound policy definitions are supported for this platform.)</td>
</tr>
<tr>
<td>Class Members</td>
<td>The class that is a member of the policy.</td>
</tr>
</tbody>
</table>

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign Queue</td>
<td>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.</td>
</tr>
<tr>
<td>Class Name</td>
<td>The name of this class.</td>
</tr>
<tr>
<td>Committed Burst Size (KB)</td>
<td>The committed burst size, used in simple policing.</td>
</tr>
<tr>
<td>Committed Rate (Kbps)</td>
<td>The committed rate, used in simple policing.</td>
</tr>
<tr>
<td>Conform Action</td>
<td>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.</td>
</tr>
<tr>
<td>Conform Color Mode</td>
<td>The current setting for the color mode. Policing uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome.</td>
</tr>
<tr>
<td>Conform COS</td>
<td>The CoS mark value if the conform action is set-cos-transmit.</td>
</tr>
<tr>
<td>Conform DSCP Value</td>
<td>The DSCP mark value if the conform action is set-dscp-transmit.</td>
</tr>
<tr>
<td>Conform IP Precedence Value</td>
<td>The IP Precedence mark value if the conform action is set-prec-transmit.</td>
</tr>
<tr>
<td>Drop</td>
<td>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.</td>
</tr>
<tr>
<td>Exceed Action</td>
<td>The action taken on traffic that exceeds settings that the network administrator specifies.</td>
</tr>
<tr>
<td>Exceed Color Mode</td>
<td>The current setting for the color of exceeding traffic that the user may optionally specify.</td>
</tr>
<tr>
<td>Mark CoS</td>
<td>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.</td>
</tr>
<tr>
<td>Mark CoS as Secondary CoS</td>
<td>The secondary 802.1p priority value (second/inner VLAN tag. Same as CoS (802.1p) marking, but the dot1p value used for remarking is picked from the dot1p value in the secondary (i.e. inner) tag of a double-tagged packet.</td>
</tr>
<tr>
<td>Mark IP DSCP</td>
<td>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.</td>
</tr>
<tr>
<td>Mark IP Precedence</td>
<td>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.</td>
</tr>
<tr>
<td>Mirror</td>
<td>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.</td>
</tr>
<tr>
<td>Non-Conform Action</td>
<td>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.</td>
</tr>
<tr>
<td>Non-Conform COS</td>
<td>The CoS mark value if the non-conform action is set-cos-transmit.</td>
</tr>
<tr>
<td>Non-Conform DSCP Value</td>
<td>The DSCP mark value if the non-conform action is set-dscp-transmit.</td>
</tr>
<tr>
<td>Non-Conform IP Precedence Value</td>
<td>The IP Precedence mark value if the non-conform action is set-prec-transmit.</td>
</tr>
</tbody>
</table>
If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

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

**Example:** The following shows example CLI display output including the mark-cos-as-sec-cos option specified in the policy action.

(FASTPATH Routing) #show policy-map p1  
Policy Name............................... p1  
Policy Type.................................. In  
Class Name.................................. c1  
Mark CoS as Secondary CoS............... Yes

**Example:** The following shows example CLI display output including the mark-cos-as-sec-cos action used in the policing (simple-police, police-single-rate, police two-rate) command.

(FASTPATH Routing) #show policy-map p2  
Policy Name............................... p2  
Policing Style......................... In  
Class Name.................................. c2  
Committed Rate.................. 1  
Committed Burst Size........... 1  
Peak Rate............................. 1  
Peak Burst Size.................. 1  
Conform Action..................... Mark CoS as Secondary CoS  
Exceed Action....................... Mark CoS as Secondary CoS  
Non-Conform Action............. Mark CoS as Secondary CoS  
Conform Color Mode............ Blind  
Exceed Color Mode............. Blind

### 7.6.4 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
7.6.5  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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiffServ Admin Mode</td>
<td>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.</td>
</tr>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Direction</td>
<td>The traffic direction of this interface service.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The current operational status of this DiffServ service interface.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The name of the policy attached to the interface in the indicated direction.</td>
</tr>
<tr>
<td>Policy Details</td>
<td>Attached policy details, whose content is identical to that described for the show policy-map policymapname command (content not repeated here for brevity).</td>
</tr>
</tbody>
</table>

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Direction</td>
<td>The traffic direction of this interface service.</td>
</tr>
<tr>
<td>OperStatus</td>
<td>The current operational status of this DiffServ service interface.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The name of the policy attached to the interface in the indicated direction.</td>
</tr>
</tbody>
</table>

7.6.6  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. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number.

This command is only allowed while the DiffServ administrative mode is enabled.

Format  show policy-map interface slot/port [in]
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Direction</td>
<td>The traffic direction of this interface service.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The current operational status of this DiffServ service interface.</td>
</tr>
</tbody>
</table>
The following information is repeated for each class instance within this policy:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>The name of the policy attached to the interface in the indicated direction.</td>
</tr>
</tbody>
</table>

7.6.7 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):

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The current operational status of this DiffServ service interface.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The name of the policy attached to the interface.</td>
</tr>
</tbody>
</table>

7.7 MAC Access Control List Commands

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

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- For the Broadcom 5630x platform, if you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

7.7.1 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. The rate-limit attribute configures the committed rate and the committed burst size.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Notice: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.
7.7.1.1 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

7.7.2 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

7.7.3 mac access-list resequence

Use this command to renumber the sequence numbers of the entries for specified MAC access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>starting-sequence-number</td>
<td>The sequence number from which to start. The range is 1–2147483647. The default is 10.</td>
</tr>
<tr>
<td>increment</td>
<td>The amount to increment. The range is 1–2147483647. The default is 10.</td>
</tr>
</tbody>
</table>

7.7.4 {deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. 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.

**Format**

{sequence-number} {deny|permit} {srcmac | any} {dstmac | any} [ethertypekey | 0x0600-0xFFFF] [vlan {eq 0-4095}] [cos 0-7] [[log] [time-range time-range-name] [assign-queue queue-id]] [[mirror | redirect] unit/slot/port][rate-limit rate burst-size]
The sequence-number specifies the sequence number for the ACL rule. The sequence number is specified by the user or is generated by device.

If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed in the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. A rule cannot be created that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule.

For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, the user can move the ACL rule to a different position in the ACL.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported ethertype-key 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>
<thead>
<tr>
<th>Ethertype Key</th>
<th>Corresponding Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>appletalk</td>
<td>0x809B</td>
</tr>
<tr>
<td>arp</td>
<td>0x0806</td>
</tr>
<tr>
<td>ibmsna</td>
<td>0x80D5</td>
</tr>
<tr>
<td>ipv4</td>
<td>0x0800</td>
</tr>
<tr>
<td>ipv6</td>
<td>0x8600</td>
</tr>
<tr>
<td>ipx</td>
<td>0x8037</td>
</tr>
<tr>
<td>mplsmcast</td>
<td>0x8848</td>
</tr>
<tr>
<td>mplsucast</td>
<td>0x8847</td>
</tr>
<tr>
<td>netbios</td>
<td>0x8191</td>
</tr>
<tr>
<td>novell</td>
<td>0x8137, 0x8138</td>
</tr>
<tr>
<td>pppoe</td>
<td>0x8863, 0x8864</td>
</tr>
<tr>
<td>rarp</td>
<td>0x8035</td>
</tr>
</tbody>
</table>

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 time-range parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 792.

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 unit/slot/port, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified unit/slot/port. The assign-queue and redirect parameters are only valid for a permit rule.
The `mirror` and `redirect` parameters are not available on the Broadcom 5630x platform.

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.

The permit command’s optional attribute `rate-limit` allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

**Example:** The following shows an example of the command.

```
(Routing) (Config)#mac access-list extended mac1
(Routing) (Config-mac-access-list)#permit 00:00:00:00:aa:bb ff:ff:ff:ff:00:00 any rate-limit 32 16
(Routing) (Config-mac-access-list)#exit
```

### 7.7.4.1 no sequence-number

Use this command to remove the ACL rule with the specified sequence number from the ACL.

**Format**

```
no sequence-number
```

**Mode**

MAC-Access-List Config

### 7.7.5 mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by `name` to an interface or range of interfaces, 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.

An optional `control-plane` is specified to apply the MAC ACL on CPU port. The control packets like BPDU are also dropped because of the implicit deny all rule added to the end of the list. To overcome this, permit rules must be added to allow the control packets.

The keyword `control-plane` is only available in Global Config mode.

You should be aware that the `out` option may or may not be available, depending on the platform.

**Format**

```
mac access-group name {{control-plane|in|out} vlan vlan-id {in|out}} [sequence 1-4294967295]
```

**Modes**

- Global Config
- Interface Config
Example: The following shows an example of the command.

```
(Routing)(Config)#mac access-group mac1 control-plane
```

### 7.7.5.1 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 {{control-plane|in|out} vlan vlan-id {in|out}}`

**Modes**

- Global Config
- Interface Config

Example: The following shows an example of the command.

```
(Routing)(Config)#no mac access-group mac1 control-plane
```

### 7.7.6 remark

This command adds a new comment to the ACL rule.

Use the remark keyword to add comments (remarks) to ACL rule entries belonging to an IPv4, IPv6, MAC, or ARP ACL. Up to `L7_ACL_MAX_RULES_PER_LIST*10` remarks per ACL and up to 10 remarks per ACL rule can be configured. Also, up to `L7_ACL_MAX_RULES*2` remarks for all QOS ACLs(IPv4/IPv6/MAC) for device can be configured. The total length of the remark cannot exceed 100 characters. A remark can contain characters in the range A-Z, a-z, 0-9, and special characters like space, hyphen, underscore. Remarks are associated to the ACL rule that is immediately created after the remarks are created. If the ACL rule is removed, the associated remarks are also deleted. Remarks are shown only in `show running-config` and are not displayed in `show ip access-lists`.

Remarks can only be added before creating the rule. If a user creates up to 10 remarks, each of them is linked to the next created rule.

**Default**

None

**Format**

`remark comment`

**Mode**

- IPv4-Access-List Config
- IPv6-Access-List-Config
- MAC-Access-List Config
- ARP-Access-List Config

Example:

```
(Config)#arp access-list new
(Config-arp-access-list)#remark “test1”
(Config-arp-access-list)#permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
(Config-arp-access-list)#remark “test1”
(Config-arp-access-list)#remark “test2”
(Config-arp-access-list)#remark “test3”
(Config-arp-access-list)#permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
(Config-arp-access-list)#remark “test4”
(Config-arp-access-list)#remark “test5”
(Config-arp-access-list)#permit ip host 2.1.1.3 mac host 00:03:04:05:06:01
```
### 7.7.6.1 no remark

Use this command to remove a remark from an ACL access-list. When the first occurrence of the remark in ACL is found, the remark is deleted. Repeated execution of this command with the same remark removes the remark from the next ACL rule that has the remark associated with it (if there is any rule configured with the same remark). If there are no more rules with this remark, an error message is displayed.

If there is no such remark associated with any rule and such remark is among not associated remarks, it is removed.

**Default** None

**Format** `no remark` comment

**Mode**
- IPv4-Access-List Config
- IPv6-Access-List Config
- MAC-Access-List Config
- ARP-Access-List Config

### 7.7.7 show mac access-lists

This command displays summary information for all Mac Access lists and ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented (for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, if an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/discarded packets. (For example: For a burst of 100 packets, the Counter value is 100).

If the ACL rule is configured with RATE LIMIT, the counter value is the MATCHED packet count. If the sent traffic rate exceeds the configured limit, the counters still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) which would equal the sent rate. For example, if rate limit is set to 10 kbps and ‘matching’ traffic is sent at 100 kbps, counters reflect a 100 kbps value. If the sent traffic rate is less than the configured limit, counters display only the matched packet count. Either way, only the matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

Use the access list name to display detailed information of a specific MAC ACL.

---

**Notice**

The command output varies based on the match criteria configured within the rules of an ACL.

---

**Format** `show mac access-lists [name]`

**Mode** Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Name</td>
<td>The user-configured name of the ACL.</td>
</tr>
<tr>
<td>ACL Counters</td>
<td>Identifies whether the ACL counters are enabled or disabled.</td>
</tr>
<tr>
<td>Interface(s)</td>
<td>The inbound or outbound interfaces to which the ACL is applied.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The ordered rule number identifier defined within the MAC ACL.</td>
</tr>
<tr>
<td>Action</td>
<td>The action associated with each rule. The possible values are Permit or Deny.</td>
</tr>
<tr>
<td>Source MAC Address</td>
<td>The source MAC address for this rule.</td>
</tr>
<tr>
<td>Source MAC Mask</td>
<td>The source MAC mask for this rule.</td>
</tr>
<tr>
<td>Committed Rate</td>
<td>The committed rate defined by the rate-limit attribute.</td>
</tr>
</tbody>
</table>
### Example: The following shows example CLI display output for the command.

(Routing) #show mac access-lists mac1

ACL Name: mac1
ACL Counters: Enabled

Outbound Interface(s): control-plane

<table>
<thead>
<tr>
<th>Sequence Number</th>
<th>Action</th>
<th>Source MAC Address</th>
<th>Source MAC Mask</th>
<th>Committed Rate</th>
<th>Committed Burst Size</th>
<th>ACL Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>permit</td>
<td>00:00:00:00:AA:BB</td>
<td>FF:FF:FF:FF:00:00</td>
<td>32</td>
<td>16</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sequence Number</th>
<th>Action</th>
<th>Source MAC Address</th>
<th>Source MAC Mask</th>
<th>Destination MAC Address</th>
<th>Destination MAC Mask</th>
<th>Ethertype</th>
<th>VLAN</th>
<th>CoS Value</th>
<th>Assign Queue</th>
<th>Redirect Interface</th>
<th>Committed Rate</th>
<th>Committed Burst Size</th>
<th>ACL Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>permit</td>
<td>00:00:00:00:AA:BB</td>
<td>FF:FF:FF:FF:00:00</td>
<td>01:80:C2:00:00:00</td>
<td>00:00:00:FF:FF:FF</td>
<td>ipv6</td>
<td>36</td>
<td>7</td>
<td>4</td>
<td>0/34</td>
<td>32</td>
<td>16</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committed Burst Size</td>
<td>The committed burst size defined by the rate-limit attribute.</td>
</tr>
<tr>
<td>Destination MAC Address</td>
<td>The destination MAC address for this rule.</td>
</tr>
<tr>
<td>Ethertype</td>
<td>The Ethertype keyword or custom value for this rule.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN identifier value or range for this rule.</td>
</tr>
<tr>
<td>COS</td>
<td>The COS (802.1p) value for this rule.</td>
</tr>
<tr>
<td>Log</td>
<td>Displays when you enable logging for the rule.</td>
</tr>
<tr>
<td>Assign Queue</td>
<td>The queue identifier to which packets matching this rule are assigned.</td>
</tr>
<tr>
<td>Redirect Interface</td>
<td>On Broadcom 5650x platforms, the unit/slot/port to which packets matching this rule are copied.</td>
</tr>
<tr>
<td>Time Range Name</td>
<td>Displays the name of the time-range if the MAC ACL rule has referenced a time range.</td>
</tr>
<tr>
<td>Rule Status</td>
<td>Status (Active/Inactive) of the MAC ACL rule.</td>
</tr>
<tr>
<td>ACL Hit Count</td>
<td>The ACL rule hit count of packets matching the configured ACL rule within an ACL.</td>
</tr>
</tbody>
</table>
7.8 IP Access Control List Commands

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

The following rules apply to IP ACLs:

- FASTPATH software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- On Broadcom 5630x platforms, if you configure a MAC ACL on an interface, you cannot configure an IP ACL on the same interface.
-Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1’s) in the bit positions that are used for the network address, and has zeros (0’s) for the bit positions that are not used. In contrast, a wildcard mask has (0’s) in a bit position that must be checked. A 1 in a bit position of the ACL mask indicates the corresponding bit can be ignored.

7.8.1 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 14 describes the parameters for the access-list command.

**IP Standard ACL:**

```
Format: access-list 1-99 [remark comment] | [{sequence-number}] [rule 1-1023] {deny | permit} {every | srcip srcmask | host srcip} [time-range time-range-name] [log] [assign-queue queue-id] [[mirror | redirect] unit/slot/port] [rate-limit rate burst-size]
```

**Mode:** Global Config

**IP Extended ACL:**

```
Format: access-list 100-199 [remark comment] | [{sequence-number}] [rule 1-1023] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0-255} | srcip srcmask|any|host srcip}|range (portkey|startport) (portkey|endport) [eq | neq | lt | gt] (portkey|0-65535) (dstip dstmask|any|host dstip)|range (portkey|startport) (portkey|endport) | (eq | neq | lt | gt) (portkey | 0-65535) | [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type icmp-type | icmp-code icmp-code] | icmp-message icmp-type | [fragments] [precedence precedence | tos tos | tosmask | dscp dscp] | [time-range time-range-name] [log] [assign-queue queue-id] [[mirror | redirect] unit/slot/port] [rate-limit rate burst-size]
```

**Mode:** Global Config

---

**NOTICE** IPv4 extended ACLs have the following limitations for egress ACLs:

- Match on port ranges is not supported.
- The rate-limit command is not supported.
### Table 14: ACL Command Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remark comment</td>
<td>Use the remark keyword to add a comment (remark) to an IP standard or IP extended ACL. The remarks make the ACL easier to understand and scan. Each remark is limited to 100 characters. A remark can consist of characters in the range A-Z, a-z, 0-9, and special characters: space, hyphen, underscore. Remarks are displayed only in show running configuration. One remark per rule can be added for IP standard or IP extended ACL. User can remove only remarks that are not associated with a rule. Remarks associated with a rule are removed when the rule is removed.</td>
</tr>
<tr>
<td>sequence-number</td>
<td>Specifies a sequence number for the ACL rule. Every rule receives a sequence number. A sequence number is specified by the user or is generated by the device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in the ACL is used and this rule is located in the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. It is not allowed to create a rule that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule. For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, user can move the ACL rule to a different position in the ACL.</td>
</tr>
<tr>
<td>1-99 or 100-199</td>
<td>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.</td>
</tr>
<tr>
<td>[rule 1-1023]</td>
<td>Specifies the IP access list rule. Specifies whether the IP ACL rule permits or denies an action. <strong>Note:</strong> For 5630x and 5650x-based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect. Match every packet. Specifies the protocol to filter for an extended IP ACL rule. Specifies a source IP address and source netmask for match condition of the IP ACL rule. Specifying any specifies <code>srcip</code> as 0.0.0.0 and <code>srcmask</code> as 255.255.255.255. Specifying host A.B.C.D specifies <code>srcip</code> as A.B.C.D and <code>srcmask</code> as 0.0.0.0.</td>
</tr>
</tbody>
</table>
Table 14: ACL Command Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| {range(portkey|startport)|{portkey | }-65535} | Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the portkey, which can be one of the following keywords:  
  - For UDP: domain, echo, ntp, rip, snmp, tftp, time, and who.  
For both TCP and UDP, each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range. If range is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified portrange. The startport and endport parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When eq is specified, the IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>. When gt is specified, the IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When neq is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to <specified port number – 1> and one with range equal to <<specified port number + 1 to 65535>>. Port number matches only apply to unfragmented or first fragments.  

| dstip dstmask|any|host dstip | Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying dstip as 0.0.0.0 and dstmask as 255.255.255.255. Specifying host A.B.C.D implies dstip as A.B.C.D and dstmask as 0.0.0.0.  

| [precedence precedence | tos tos | [tosmask] | dscp dscp] | Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters dscp, precedence, tos/tosmask.  
  
  Note: tosmask is an optional parameter.  

| flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established] | Specifies that the IP ACL rule matches on the TCP flags. When +<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is set in the TCP header. When –<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is “NOT” set in the TCP header. When established is specified, a match occurs if the specified RST or ACK bits are set in the TCP header. Two rules are installed in the hardware when the established option is specified.  
  
  Note: This option is available only if the protocol is tcp.  

Note: This option is available only if the protocol is TCP or UDP.
Table 14: ACL Command Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[icmp-type icmp-type [icmp-code icmp-code]</td>
<td>Note: This option is available only if the protocol is icmp. Specifies a match condition for ICMP packets. When icmp-type is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When icmp-code is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying icmp-message implies that both icmp-type and icmp-code are specified. The following icmp-messages are supported: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded and unreachable.</td>
</tr>
<tr>
<td>igmp-type igmp-type</td>
<td>This option is available only if the protocol is igmp. When igmp-type is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.</td>
</tr>
<tr>
<td>fragments</td>
<td>Specifies that the IP ACL rule matches on fragmented IP packets.</td>
</tr>
<tr>
<td>[log]</td>
<td>Specifies that this rule is to be logged.</td>
</tr>
<tr>
<td>[time-range time-range-name]</td>
<td>Allows imposing time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see &quot;Time Range Commands for Time-Based ACLs&quot; on page 792.</td>
</tr>
<tr>
<td>[assign-queue queue-id]</td>
<td>Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.</td>
</tr>
<tr>
<td>[[mirror</td>
<td>redirect] slot/port]</td>
</tr>
<tr>
<td>[rate-limit rate burst-size]</td>
<td>Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.</td>
</tr>
</tbody>
</table>
7.8.1 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 [rule 1-1023]
Mode    Global Config

7.8.2 access-list counters enable
Use this command to enable ACL counters for IPv4, IPv6 and MAC access lists.

Default  Enabled
Format    access-list counters enable
Mode      Global Config

7.8.2.1 no access-list counters enable
Use this command to disable ACL counters for IPv4, IPv6 and MAC access lists.

Format    no access-list counters enable
Mode      Global Config

7.8.3 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. The rate-limit attribute configures the committed rate and the committed burst size.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

---

**NOTICE**

The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format    ip access-list name
Mode      Global Config
7.8.3.1  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

7.8.4  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

7.8.5  ip access-list resequence
Use this command to renumber the sequence numbers of the entries for specified IP access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

**Default**
10

**Format**
```
ip access-list resequence {name | id} starting-sequence-number increment
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>starting-sequence-number</td>
<td>The sequence number from which to start. The range is 1–2147483647. The default is 10.</td>
</tr>
<tr>
<td>increment</td>
<td>The amount to increment. The range is 1–2147483647. The default is 10.</td>
</tr>
</tbody>
</table>

7.8.6  {deny | permit} (IP ACL)
This command creates a new rule for the current IP 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 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 time-range parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 792.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed queue-id value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The assign-queue parameter is valid only for a permit rule.

The permit command's optional attribute rate-limit allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence-number</td>
<td>The sequence-number specifies the sequence number for the ACL rule. The sequence number is specified by the user or is generated by device.</td>
</tr>
<tr>
<td></td>
<td>If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed at the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. A rule cannot be created that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule. For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, the user can move the ACL rule to a different position in the ACL.</td>
</tr>
<tr>
<td>{deny</td>
<td>permit}</td>
</tr>
<tr>
<td>Every</td>
<td>Match every packet.</td>
</tr>
<tr>
<td>[eigrp</td>
<td>gre</td>
</tr>
<tr>
<td>srcip srcmask</td>
<td>any</td>
</tr>
<tr>
<td></td>
<td>Specifying “any” implies specifying srcip as “0.0.0.0” and srcmask as “255.255.255.255”.</td>
</tr>
<tr>
<td></td>
<td>Specifying “host A.B.C.D” implies srcip as “A.B.C.D” and srcmask as “0.0.0.0”.</td>
</tr>
</tbody>
</table>
### Parameters

{{range (portkey | startport | endport) | eq | neq | lt | gt) (portkey | 0-65535) }}

#### Note:
This option is available only if the protocol is tcp or udp.

Specifies the layer 4 port match condition for the IP ACL rule. Port number can be used, which ranges from 0-65535, or the portkey, which can be one of the following keywords:

- For tcp protocol: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3
- For udp protocol: domain, echo, ntp, rip, snmp, tftp, time, who

Each of these keywords translates into its equivalent port number.

When range is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified port range. The startport and endport parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal to or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range.

When eq is specified, IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey.

When lt is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number - 1>.

When gt is specified, IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535.

When neq is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to <specified port number _- 1> and one with range equal to <specified port number _+ 1 to 65535>.

Port number matches only apply to unfragmented or first fragments.

### dstip dstmask | any | host dstip

Specifies a destination IP address and netmask for match condition of the IP ACL rule.

Specifying any implies specifying dstip as 0.0.0.0 and dstmask as 255.255.255.255.

Specifying host A.B.C.D implies dstip as A.B.C.D and dstmask as 0.0.0.0.

### [precedence precedence] | tos tos [tosmask] | dscp dscp

Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters dscp, precedence, tos/tosmask. tosmask is an optional parameter.

### flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]

Specifies that the IP ACL rule matches on the tcp flags.

When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header.

When -<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is NOT set in the TCP header.

When established is specified, a match occurs if either the specified RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when the established option is specified.

This option is available only if protocol is tcp.
Example: The following shows an example of the command.

(Routing) (Config)#ip access-list ip1

(Routing) (Config-ipv4-acl)#permit icmp any any rate-limit 32 16

(Routing) (Config-ipv4-acl)#exit
7.8.6.1 no sequence-number

Use this command to remove the ACL rule with the specified sequence number from the ACL.

**Format**

```
no sequence-number
```

**Mode**

Ipv4-Access-List Config

7.8.7 ip access-group

This command either attaches a specific IP Access Control List (ACL) identified by `accesslistnumber` or `name` to an interface, range of interfaces, or all interfaces; or associates it with a VLAN ID in a given direction. The parameter `name` is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

An optional `control-plane` is specified to apply the ACL on CPU port. The IPv4 control packets like RADIUS and TACACS+ are also dropped because of the implicit deny all rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv4 control packets.

---

**NOTICE**

The keyword `control-plane` is only available in Global Config mode.

---

**NOTICE**

You should be aware that the `out` option may or may not be available, depending on the platform.

---

**Default**

none

**Format**

```
ip access-group {accesslistnumber|name} {{control-plane|in|out}|vlan vlan-id} {in|out} [sequence 1-4294967295]
```

**Modes**

- Interface Config
- Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accesslistnumber</td>
<td>Identifies a specific IP ACL. The range is 1 to 199.</td>
</tr>
<tr>
<td>sequence</td>
<td>A optional sequence number that indicates the order of this IP access list relative to the other IP access lists already assigned to this interface and direction. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>A VLAN ID associated with a specific IP ACL in a given direction.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the Access Control List.</td>
</tr>
</tbody>
</table>

**Example:** The following shows an example of the command.

(Routing) (Config)#ip access-group ip1 control-plane
7.8.7.1 no ip access-group
This command removes a specified IP ACL from an interface.

Default none
Format no ip access-group {accesslistnumber|name} {control-plane|in|out}|vlan vlan-id {in|out}
Mode • Interface Config
• Global Config

Example: The following shows an example of the command.
(Routing)(Config)#no ip access-group ip1 control-plane

7.8.8 acl-trapflags
This command enables the ACL trap mode.

Default disabled
Format acl-trapflags
Mode Global Config

7.8.8.1 no acl-trapflags
This command disables the ACL trap mode.

Format no acl-trapflags
Mode Global Config

7.8.9 show ip access-lists
Use this command to view summary information about all IP ACLs configured on the switch. To view more
detailed information about a specific access list, specify the ACL number or name that is used to identify the IP
ACL. It displays committed rate, committed burst size, and ACL rule hit count of packets matching the
configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a
dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get
incremented for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be
incremented).

For ACL counters, if an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/discarded
packets (for example: If burst of 100 packets sent from IXIA, the Counter value is 100).

If an ACL rule is configured with RATE LIMIT, the counter value will be the MATCHED packet count. If the sent traffic rate
exceeds the configured limit, counters will still display matched packet count (despite getting dropped beyond the con-
figured limit since match criteria is met) that would equal the sent rate. For example, if rate limit is set to 10 kbps and
'matching' traffic is sent at 100 kbps, counters would reflect 100 kbps value. If the sent traffic rate is less than the config-
ured limit, counters would display only matched packet count. Either way, only matched packet count is reflected in the
counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

Format show ip access-lists [accesslistnumber | name]
Mode Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Counters</td>
<td>Shows whether ACL counters are enabled or disabled.</td>
</tr>
</tbody>
</table>
If you specify an IP ACL number or name, the following information displays:

**Notice**: Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current number of ACLs</td>
<td>The number of ACLs of any type currently configured on the system.</td>
</tr>
<tr>
<td>Maximum number of ACLs</td>
<td>The maximum number of ACLs of any type that can be configured on the system.</td>
</tr>
<tr>
<td>ACL ID/Name</td>
<td>Identifies the configured ACL number or name.</td>
</tr>
<tr>
<td>Rules</td>
<td>Identifies the number of rules configured for the ACL.</td>
</tr>
<tr>
<td>Direction</td>
<td>Shows whether the ACL is applied to traffic coming into the interface (inbound/ingress) or leaving the interface (outbound/egress).</td>
</tr>
<tr>
<td>Interface(s)</td>
<td>The interface(s) to which the ACL is applied (ACL interface bindings).</td>
</tr>
<tr>
<td>VLAN(s)</td>
<td>The VLANs to which the ACL is applied (ACL VLAN bindings).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL ID</td>
<td>The user-configured ACL identifier.</td>
</tr>
<tr>
<td>ACL Counters</td>
<td>Identifies whether the ACL counters are enabled or disabled.</td>
</tr>
<tr>
<td>Interface(s)</td>
<td>The inbound or outbound interfaces to which the ACL is applied.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The number identifier for each rule that is defined for the IP ACL.</td>
</tr>
<tr>
<td>Action</td>
<td>The action associated with each rule. The possible values are Permit or Deny.</td>
</tr>
<tr>
<td>Match All</td>
<td>Indicates whether this access list applies to every packet. Possible values are True or False.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol to filter for this rule.</td>
</tr>
<tr>
<td>ICMP Type</td>
<td><strong>Note</strong>: This is shown only if the protocol is ICMP. The ICMP message type for this rule.</td>
</tr>
<tr>
<td>Starting Source L4 port</td>
<td>The starting source layer 4 port.</td>
</tr>
<tr>
<td>Ending Source L4 port</td>
<td>The ending source layer 4 port.</td>
</tr>
<tr>
<td>Starting Destination L4 port</td>
<td>The starting destination layer 4 port.</td>
</tr>
<tr>
<td>Ending Destination L4 port</td>
<td>The ending destination layer 4 port.</td>
</tr>
<tr>
<td>ICMP Code</td>
<td><strong>Note</strong>: This is shown only if the protocol is ICMP. The ICMP message code for this rule.</td>
</tr>
<tr>
<td>Fragments</td>
<td>If the ACL rule matches on fragmented IP packets.</td>
</tr>
<tr>
<td>Committed Rate</td>
<td>The committed rate defined by the rate-limit attribute.</td>
</tr>
<tr>
<td>Committed Burst Size</td>
<td>The committed burst size defined by the rate-limit attribute.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>The source IP address for this rule.</td>
</tr>
<tr>
<td>Source IP Mask</td>
<td>The source IP Mask for this rule.</td>
</tr>
<tr>
<td>Source L4 Port Keyword</td>
<td>The source port for this rule.</td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>The destination IP address for this rule.</td>
</tr>
<tr>
<td>Destination IP Mask</td>
<td>The destination IP Mask for this rule.</td>
</tr>
<tr>
<td>Destination L4 Port Keyword</td>
<td>The destination port for this rule.</td>
</tr>
<tr>
<td>IP DSCP</td>
<td>The value specified for IP DSCP.</td>
</tr>
<tr>
<td>IP Precedence</td>
<td>The value specified IP Precedence.</td>
</tr>
<tr>
<td>IP TOS</td>
<td>The value specified for IP TOS.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(Routing) #show ip access-lists ip1

ACL Name: ip1
ACL Counters: Enabled
Inbound Interface(s): 1/0/30

Sequence Number: 1
Action............................................ permit
Match All......................................... FALSE
Protocol......................................... 1(icmp)
ICMP Type.........................................3(Destination Unreachable)
Starting Source L4 port....................... 80
Ending Source L4 port.......................... 85
Starting Destination L4 port................... 180
Ending Destination L4 port.................... 185
ICMP Code...........................................0
Fragments........................................... FALSE
Committed Rate.................................. 32
Committed Burst Size........................... 16
ACL hit count .....................................0

7.8.10 show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction. Instead of slot/port, lag lag-intf-num can be used as an alternate way to specify the LAG interface. lag lag-intf-num can also be used to specify the LAG interface where lag-intf-num is the LAG port number. Use the control-plane keyword to display the ACLs applied on the CPU port.

Format show access-lists interface {slot/port in|out | control-plane}
Mode Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragments</td>
<td>Specifies whether the IP ACL rule matches on fragmented IP packets is enabled.</td>
</tr>
<tr>
<td>TTL Field Value</td>
<td>The value specified for the TTL.</td>
</tr>
<tr>
<td>Log</td>
<td>Displays when you enable logging for the rule.</td>
</tr>
<tr>
<td>Assign Queue</td>
<td>The queue identifier to which packets matching this rule are assigned.</td>
</tr>
<tr>
<td>Mirror Interface</td>
<td>The unit/slot/port to which packets matching this rule are copied.</td>
</tr>
<tr>
<td>Redirect Interface</td>
<td>The unit/slot/port to which packets matching this rule are forwarded.</td>
</tr>
<tr>
<td>Time Range Name</td>
<td>Displays the name of the time-range if the IP ACL rule has referenced a time range.</td>
</tr>
<tr>
<td>Rule Status</td>
<td>Status (Active/Inactive) of the IP ACL rule.</td>
</tr>
<tr>
<td>ACL Hit Count</td>
<td>The ACL rule hit count of packets matching the configured ACL rule within an ACL.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Type</td>
<td>Type of access list (IP, IPv6, or MAC).</td>
</tr>
<tr>
<td>ACL ID</td>
<td>Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>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).</td>
</tr>
</tbody>
</table>
**Example:** The following shows an example of the command.

(Routing) `#show access-lists interface control-plane`

<table>
<thead>
<tr>
<th>ACL Type</th>
<th>ACL ID</th>
<th>Sequence Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6</td>
<td>ip61</td>
<td>1</td>
</tr>
</tbody>
</table>

### 7.8.11 show access-lists vlan

This command displays Access List information for a particular VLAN ID. The `vlan-id` parameter is the VLAN ID of the VLAN with the information to view. The `{in | out}` options specifies the direction of the VLAN ACL information to view.

**Format**

```
show access-lists vlan vlan-id in|out
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Type</td>
<td>Type of access list (IP, IPv6, or MAC).</td>
</tr>
<tr>
<td>ACL ID</td>
<td>Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>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).</td>
</tr>
</tbody>
</table>

### 7.8.12 acl-traptime

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. The range is 30..600, the default value is 300.

**Format**

```
acl-traptime <30-600>
```

**Mode**

Global Config
7.8.12.1 no acl-traptime
This command disables the time interval for generating ACL traps.

Format: no acl-traptime
Mode: Global Config

7.8.13 show acl-traptime
This command displays the time interval for generating ACL traps. A trap is generated if an ACL rule applies for an incoming packet.

Format: show acl-traptime
Mode: Privileged Exec

7.9 IPv6 Access Control List Commands
This section describes the commands you use to configure IPv6 Access Control List (ACL) settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:
- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

7.9.1 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. The rate-limit attribute configures the committed rate and the committed burst size.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format: ipv6 access-list name
Mode: Global Config
7.9.1.1 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

7.9.2 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

7.9.3 ipv6 access-list resequence
Use this command to renumber the sequence numbers of the entries for specified IPv6 access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default: 10

Format:  ipv6 access-list resequence {name | id } starting-sequence-number increment
Mode:   Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>starting-sequence-number</td>
<td>The sequence number from which to start. The range is 1–2147483647. The default is 10.</td>
</tr>
<tr>
<td>increment</td>
<td>The amount to increment. The range is 1–2147483647. The default is 10.</td>
</tr>
</tbody>
</table>

7.9.4 {deny | permit} (IPv6)
This command creates a new rule for the current IPv6 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 time-range parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see "Time Range Commands for Time-Based ACLs" on page 792.

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 unit/slot/port, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified unit/slot/port. The assign-queue and redirect parameters are only valid for a permit rule.

The mirror and redirect parameters are not available on the Broadcom 5630x platform.

The permit command's optional attribute rate-limit allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

IPv6 ACLs have the following limitations:

- Port ranges are not supported for egress IPv6 ACLs.
- For BCM5684X platforms, the IPv6 ACL routing keyword is not supported when an IPv6 address is specified.
- For BCM5684X and BCM5644X platforms, the IPv6 ACL fragment keyword matches only on the first two IPv6 extension headers for the fragment header (next header code 44). If the fragment header appears in the third or subsequent header, it is not matched.
- For platforms other than BCM5684X and BCM5644X, the IPv6 ACL fragment keyword matches only on the first IPv6 extension header (next header code 44). If the fragment header appears in the second or subsequent header, it is not matched.
- For platforms other than the BCM5644X, the IPv6 ACL routing keyword matches only on the first IPv6 extension header (next header code 43). If the fragment header appears in the second or subsequent header, it is not matched.
- The rate-limit command is not supported for egress IPv6 ACLs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{deny</td>
<td>permit}</td>
</tr>
<tr>
<td>Every</td>
<td>Specifies to match every packet.</td>
</tr>
<tr>
<td>{protocolkey</td>
<td>number}</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| `source-ipv6-prefix/prefix-length | any | host source-ipv6-address` | Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule.  
Specifying any implies specifying `::/0`  
Specifying `host source-ipv6-address` implies matching the specified IPv6 address.  
This `source-ipv6-address` argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| `{range {portkey | startport} (portkey | endport) | {eq | neq | lt | gt} {portkey | 0-65535 } }` | Note: This option is available only if the protocol is TCP or UDP.  
Specifies the layer 4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0-65535, or the `portkey`, which can be one of the following keywords:  
• For TCP: `bgp`, `domain`, `echo`, `ftp`, `ftp-data`, `http`, `smtp`, `telnet`, `www`, `pop2`, `pop3`  
• For UDP: `domain`, `echo`, `ntp`, `rip`, `snmp`, `tftp`, `time`, `who`.  
Each of these keywords translates into its equivalent port number.  
When range is specified, IPv6 ACL rule matches only if the layer 4 port number falls within the specified port range. The `startport` and `endport` parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between are part of the layer 4 port range.  
When `eq` is specified, IPv6 ACL rule matches only if the layer 4 port number is equal to the specified port number or `portkey`.  
When `lt` is specified, IPv6 ACL rule matches if the layer 4 port number is less than the specified port number or `portkey`. It is equivalent to specifying the range as 0 to `<specified port number - 1>`.  
When `gt` is specified, IPv6 ACL rule matches if the layer 4 port number is greater than the specified port number or `portkey`. It is equivalent to specifying the range as `<specified port number + 1>` to 65535.  
When `neq` is specified, IPv6 ACL rule matches only if the layer 4 port number is not equal to the specified port number or `portkey`.  
Two rules are added in the hardware one with range equal to 0 to `<specified port number - 1>` and one with range equal to `<specified port number + 1>` to 65535. |
| `destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address` | Specifies a destination IPv6 source address and prefix length to match for the IPv6 ACL rule.  
Specifying any implies specifying `::/0`  
Specifying `host destination-ipv6-address` implies matching the specified IPv6 address.  
This `destination-ipv6-address` argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
sequence sequence-number

Specifies a sequence number for the ACL rule. Every rule receives a sequence number. The sequence number is specified by the user or is generated by the device.

If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed at the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. It is not allowed to create a rule that duplicates an already existing one. A rule cannot be configured with a sequence number that is already used for another rule.

For example, if a user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, user can move the ACL rule to a different position in the ACL.

[dscp dscp]

Specifies the dscp value to match for for the IPv6 rule.

flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]

 Specifies that the IPv6 ACL rule matches on the tcp flags.

When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header.

When "<tcpflagname>" is specified, a match occurs if specified <tcpflagname> flag is "NOT" set in the TCP header.

When established is specified, a match occurs if specified either RST or ACK bits are set in the TCP header.

Two rules are installed in hardware when "established" option is specified.

This option is visible only if protocol is "tcp".

[icmp-type icmp-type [icmp-code icmp-code] / icmp-message icmp-message]

Note: This option is available only if the protocol is icmpv6.

Specifies a match condition for ICMP packets.

When icmp-type is specified, IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255.

When icmp-code is specified, IPv6 ACL rule matches on the specified ICMP message code, a number from 0 to 255.

Specifying icmp-message implies both icmp-type and icmp-code are specified. The following icmp-messages are supported: destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, router-renumbering, time-exceeded, and unreachable.

The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type.

Fragments

Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (Packets that have the next header field is set to 44).

Routing

Specifies that IPv6 ACL rule matches on IPv6 packets that have routing extension headers (the next header field is set to 43).
Example: The following shows an example of the command.

```
(Routing) (Config)#ipv6 access-list ip61

(Routing) (Config-ipv6-acl)#permit udp any any rate-limit 32 16

(Routing) (Config-ipv6-acl)#exit
```

### 7.9.4.1 no sequence-number

Use this command to remove the ACL rule with the specified sequence number from the ACL.

**Format**

```
no sequence-number
```

**Mode**

IPv6-Access-List Config

### 7.9.5 ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by name to an interface or range of interfaces, or associates it 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.

An optional control-plane is specified to apply the ACL on CPU port. The IPv6 control packets like IGMPv6 are also dropped because of the implicit deny all rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv6 control packets.

The keyword control-plane is only available in Global Config mode.

You should be aware that the out option may or may not be available, depending on the platform.
Example: The following shows an example of the command.

```
(Routing)(Config)#ipv6 traffic-filter ip61 control-plane
```

### 7.9.5.1 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>{{control-plane | in | out} | vlan <vlan-id} {in|out}}
```

**Modes**

- Global Config
- Interface Config

Example: The following shows an example of the command.

```
(Routing) (Config)#no ipv6 traffic-filter ip61 control-plane
```

### 7.9.6 show ipv6 access-lists

This command displays summary information of all the IPv6 Access lists. Use the access list `name` to display detailed information of a specific IPv6 ACL.

This command displays information about the attributes icmp-type, icmp-code, fragments, routing, tcp flags, and source and destination L4 port ranges. It displays committed rate, committed burst size, and ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented (for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, if an ACL rule is configured without RATE-LIMIT, the counter value is a count of the forwarded/disen-carded packets. (For example: for a burst of 100 packets, the Counter value is 100).

If an ACL rule is configured with RATE LIMIT, the counter value is that of the MATCHED packet count. If the sent traffic rate exceeds the configured limit, the counters still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) that equals the sent rate. For example, if the rate limit is set to 10 Kbps and 'matching' traffic is sent at 100 Kbps, counters would reflect 100 Kbps value. If the sent traffic rate is less than the configured limit, the counters display only the matched packet count. Either way, only the matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with DiffServ policies.

**Format**

```
show ipv6 access-lists [name]
```

**Mode**

- Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Counters</td>
<td>Shows whether ACL counters are enabled or disabled.</td>
</tr>
<tr>
<td>Current number of all ACLs</td>
<td>The number of ACLs of any type currently configured on the system.</td>
</tr>
<tr>
<td>Maximum number of all ACLs</td>
<td>The number of ACLs of any type that can be configured on the system.</td>
</tr>
<tr>
<td>IPv6 ACL Name</td>
<td>The configured ACL name.</td>
</tr>
<tr>
<td>Rules</td>
<td>The number of rules configured for the ACL.</td>
</tr>
<tr>
<td>Direction</td>
<td>Shows whether the ACL is applied to traffic coming into the interface (inbound/ingress) or leaving the interface (outbound/egress).</td>
</tr>
<tr>
<td>Interface(s)</td>
<td>Identifies the interface(s) to which the ACL is applied (ACL interface bindings).</td>
</tr>
</tbody>
</table>
If you specify an IPv6 ACL name, the following information displays:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN(s)</td>
<td>Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).</td>
</tr>
</tbody>
</table>

Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Name</td>
<td>The user-configured name of the ACL.</td>
</tr>
<tr>
<td>ACL Counters</td>
<td>Identifies whether the ACL counters are enabled or disabled.</td>
</tr>
<tr>
<td>Interface(s)</td>
<td>The inbound and/or outbound interfaces to which the ACL is applied.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The ordered rule number identifier defined within the IPv6 ACL.</td>
</tr>
<tr>
<td>Action</td>
<td>The action associated with each rule. The possible values are Permit or Deny.</td>
</tr>
<tr>
<td>Match Every</td>
<td>Indicates whether this access list applies to every packet. Possible values are True or False.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol to filter for this rule.</td>
</tr>
<tr>
<td>Committed Rate</td>
<td>The committed rate defined by the rate-limit attribute.</td>
</tr>
<tr>
<td>Committed Burst Size</td>
<td>The committed burst size defined by the rate-limit attribute.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>The source IP address for this rule.</td>
</tr>
<tr>
<td>Source L4 Port Keyword</td>
<td>The source port for this rule.</td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>The destination IP address for this rule.</td>
</tr>
<tr>
<td>Destination L4 Port Keyword</td>
<td>The destination port for this rule.</td>
</tr>
<tr>
<td>IP DSCP</td>
<td>The value specified for IP DSCP.</td>
</tr>
<tr>
<td>Log</td>
<td>Displays when you enable logging for the rule.</td>
</tr>
<tr>
<td>Assign Queue</td>
<td>The queue identifier to which packets matching this rule are assigned.</td>
</tr>
<tr>
<td>Mirror Interface</td>
<td>The unit/slot/port to which packets matching this rule are copied.</td>
</tr>
<tr>
<td>Redirect Interface</td>
<td>The unit/slot/port to which packets matching this rule are forwarded.</td>
</tr>
<tr>
<td>Time Range Name</td>
<td>Displays the name of the time-range if the IPv6 ACL rule has referenced a time range.</td>
</tr>
<tr>
<td>Rule Status</td>
<td>Status (Active/Inactive) of the IPv6 ACL rule.</td>
</tr>
<tr>
<td>ACL Hit Count</td>
<td>The ACL rule hit count of packets matching the configured ACL rule within an ACL.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(Routing) #show ipv6 access-lists ip61

ACL Name: ip61
ACL Counters: Enabled

Outbound Interface(s): control-plane

Rule Number: 1
Action........................................ permit
Match Every.................................... FALSE
Protocol....................................... 17(udp)
Committed Rate................................ 32
Committed Burst Size......................... 16
ACL hit count .................................. 0

### 7.10 Time Range Commands for Time-Based ACLs

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit deny all rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined within an ACL.

#### 7.10.1 time-range

Use this command to create a time range identified by `name`, consisting of one absolute time entry and/or one or more periodic time entries. The `name` parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries.

---

**NOTICE**

When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

**Format**

time-range name

**Mode**

Global Config

#### 7.10.1.1 no time-range

This command deletes a time-range identified by `name`.

**Format**

no time-range name

**Mode**

Global Config
7.10.2 absolute

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The time parameter is based on the currently configured time zone.

The [start time date] parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The [end time date] parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format absolute [start time date] [end time date]
Mode Time-Range Config

7.10.2.1 no absolute

This command deletes the absolute time entry in the time range

Format no absolute
Mode Time-Range Config

7.10.3 periodic

Use this command to add a periodic time entry to a time range. The time parameter is based off of the currently configured time zone.

The first occurrence of the days-of-the-week argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted.

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:
- daily—Monday through Sunday
- weekdays—Monday through Friday
- weekend—Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

The first occurrence of the time argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Format periodic days-of-the-week time to time
Mode Time-Range Config
7.10.3.1 no periodic
This command deletes a periodic time entry from a time range.

Format: no periodic days-of-the-week time to time
Mode: Time-Range Config

7.10.4 show time-range
Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the name parameter to identify a specific time range to display. When name is not specified, all the time ranges defined in the system are displayed.

Format: show time-range [name]
Mode: Privileged EXEC

The information in the following table displays when no time range name is specified.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>The administrative mode of the time range feature on the switch</td>
</tr>
<tr>
<td>Current number of all Time Ranges</td>
<td>The number of time ranges currently configured in the system.</td>
</tr>
<tr>
<td>Maximum number of all Time Ranges</td>
<td>The maximum number of time ranges that can be configured in the system.</td>
</tr>
<tr>
<td>Time Range Name</td>
<td>Name of the time range.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the time range (active/inactive)</td>
</tr>
<tr>
<td>Periodic Entry count</td>
<td>The number of periodic entries configured for the time range.</td>
</tr>
<tr>
<td>Absolute Entry</td>
<td>Indicates whether an absolute entry has been configured for the time range (Exists).</td>
</tr>
</tbody>
</table>

7.11 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.

7.11.1 auto-voip
Use this command to configure auto VoIP mode. The supported modes are protocol-based and oui-based. Protocol-based auto VoIP prioritizes the voice data based on the layer 4 port used for the voice session. OUI-based auto VoIP prioritizes the phone traffic based on the known OUI of the phone.

When both modes are enabled, if the connected phone OUI is one of the configured OUI, then the voice data is prioritized using OUI Auto VoIP, otherwise protocol-based Auto VoIP is used to prioritize the voice data.

Active sessions are cleared if protocol-based auto VoIP is disabled on the port.
7.11.1 no auto-voip
Use the no form of the command to set the default mode.

7.11.2 auto-voip oui
Use this command to configure an OUI for Auto VoIP. The traffic from the configured OUI will get the highest priority over the other traffic. The oui-prefix is a unique OUI that identifies the device manufacturer or vendor. The OUI is specified in three octet values (each octets represented as two hexadecimal digits) separated by colons. The string is a description of the OUI that identifies the manufacturer or vendor associated with the OUI.

Default: A list of known OUIS is present.
Format: auto-voip oui oui-prefix oui-desc string
Mode: Global Config

Example: The following example shows how to add an OUI to the table.

(Routing) (Config)#auto-voip oui 00:03:6B desc "Cisco VoIP Phone"

7.11.2.1 no auto-voip oui
Use the no form of the command to remove a configured OUI prefix from the table.

Format: no auto-voip oui oui-prefix
Mode: Global Config

7.11.3 auto-voip oui-based priority
Use this command to configure the global OUI based auto VoIP priority. If the phone OUI is matches one of the configured OUI, then the priority of traffic from the phone is changed to OUI priority configured through this command. The priority-value is the 802.1p priority used for traffic that matches a value in the known OUI list. If the interface detects an OUI match, the switch assigns the traffic in that session to the traffic class mapped to this priority value. Traffic classes with a higher value are generally used for time-sensitive traffic.

Default: Highest available priority.
Format: auto-voip oui-based priority priority-value
Mode: Global Config
Example: The following example shows how to add an OUI to the table.

(Routing) (Config)#auto-voip oui 00:03:6B desc "Cisco VoIPPhone"

7.11.3.1 no auto-voip oui
Use the no form of the command to remove a configured OUI prefix from the table.

Format: no auto-voip oui oui-prefix
Mode: • Global Config
      • Interface Config

7.11.4 auto-voip protocol-based
Use this command to configure the global protocol-based auto VoIP remarking priority or traffic-class. If remark priority is configured, the voice data of the session is remarked with the priority configured through this command. The remark-priority is the 802.1p priority used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device marks traffic in that session with the specified 802.1p priority value to ensure voice traffic always gets the highest priority throughout the network path.

The tc value is the traffic class used for protocol-based VoIP traffic. If the interface detects a call-control protocol, the device assigns the traffic in that session to the configured Class of Service (CoS) queue. Traffic classes with a higher value are generally used for time-sensitive traffic. The CoS queue associated with the specified traffic class should be configured with the appropriate bandwidth allocation to allow priority treatment for VoIP traffic.

Default: Traffic class 7
Format: auto-voip protocol-based {remark remark-priority | traffic-class tc}
Mode: • Global Config
      • Interface Config

7.11.4.1 no auto-voip protocol-based
Use this command to reset the global protocol based auto VoIP remarking priority or traffic-class to the default.

Format: no auto-voip protocol-based {remark remark-priority | traffic-class tc}
Mode: • Global Config
      • Interface Config

7.11.5 auto-voip vlan
Use this command to configure the global Auto VoIP VLAN ID. The VLAN behavior is depend on the configured auto VoIP mode. The auto-VoIP VLAN is the VLAN used to segregate VoIP traffic from other non-voice traffic. All VoIP traffic that matches a value in the known OUI list gets assigned to this VoIP VLAN.
7.11.5.1 no auto-voip vlan
Use the no form of the command to reset the auto-VoIP VLAN ID to the default value.

Format: no auto-voip vlan
Mode: Global Config

7.11.6 show auto-voip
Use this command to display the auto VoIP settings on the interface or interfaces of the switch.

Format: show auto-voip {protocol-based|oui-based} interface {slot/port|all}
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP VLAN ID</td>
<td>The global VoIP VLAN ID.</td>
</tr>
<tr>
<td>Prioritization Type</td>
<td>The type of prioritization used on voice traffic.</td>
</tr>
</tbody>
</table>
| Class Value         | • If the Prioritization Type is configured as traffic-class, then this value is the queue value.  
|                     | • If the Prioritization Type is configured as remark, then this value is 802.1p priority used to re-mark the voice traffic. |
| Priority            | The 802.1p priority. This field is valid for OUI auto VoIP.                 |
| AutoVoIP Mode       | The Auto VoIP mode on the interface.                                        |

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

(Routing)# show auto-voip protocol-based interface all

VoIP VLAN ID......................... 2
Prioritization Type................. traffic-class
Class Value......................... 7

<table>
<thead>
<tr>
<th>Interface</th>
<th>Auto VoIP Mode</th>
<th>Operational Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Disabled</td>
<td>Down</td>
</tr>
<tr>
<td>0/2</td>
<td>Disabled</td>
<td>Down</td>
</tr>
<tr>
<td>0/3</td>
<td>Disabled</td>
<td>Down</td>
</tr>
<tr>
<td>0/4</td>
<td>Disabled</td>
<td>Down</td>
</tr>
</tbody>
</table>

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

(Routing)# show auto-voip oui-based interface all

VoIP VLAN Id......................... 2
Priority.............................. 7

<table>
<thead>
<tr>
<th>Interface</th>
<th>Auto VoIP Mode</th>
<th>Operational Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Disabled</td>
<td>Down</td>
</tr>
<tr>
<td>0/2</td>
<td>Disabled</td>
<td>Down</td>
</tr>
<tr>
<td>0/3</td>
<td>Disabled</td>
<td>Down</td>
</tr>
</tbody>
</table>
7.11.7 show auto-voip oui-table

Use this command to display the VoIP oui-table information.

**Format**    show auto-voip oui-table

**Mode**     Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUI</td>
<td>OUI of the source MAC address.</td>
</tr>
<tr>
<td>Status</td>
<td>Default or configured entry.</td>
</tr>
<tr>
<td>OUI Description</td>
<td>Description of the OUI.</td>
</tr>
</tbody>
</table>

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

(Routing)# show auto-voip oui-table

<table>
<thead>
<tr>
<th>OUI</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:01:E3</td>
<td>Default</td>
<td>SIEMENS</td>
</tr>
<tr>
<td>00:03:6B</td>
<td>Default</td>
<td>CISCO1</td>
</tr>
<tr>
<td>00:01:01</td>
<td>Configured</td>
<td>VoIP phone</td>
</tr>
</tbody>
</table>

7.12 iSCSI Optimization Commands

This section describes commands you use to monitor iSCSI sessions and prioritize iSCSI packets. iSCSI Optimization provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

7.12.1 iscsi aging time

This command sets the aging time for iSCSI sessions. Behavior when changing aging time:

- When aging time is increased, current sessions will be timed out according to the new value.
- When aging time is decreased, any sessions that have been dormant for a time exceeding the new setting will be immediately deleted from the table. All other sessions will continue to be monitored against the new time out value.

**Default**    10 minutes

**Format**    iscsi aging time **time**

**Mode**     Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>The number of minutes a session must be inactive prior to its removal. Range: 1-43,200.</td>
</tr>
</tbody>
</table>

**Example:** The following example sets the aging time for iSCSI sessions to 100 minutes.

(switch)(config)# iscsi aging time 100
7.12.1.1 no iscsi aging time

Use the no form of the command to reset the aging time value to the default value.

Format: no iscsi aging time
Mode: Global Config

7.12.2 iscsi cos

This command sets the quality of service profile that will be applied to iSCSI flows. iSCSI flows are assigned by default to the highest VPT/DSCP mapped to the highest queue not used for stack management. The user should also take care of configuring the relevant Class of Service parameters for the queue in order to complete the setting.

Setting the VPT/DSCP sets the QoS profile which determines the egress queue to which the frame is mapped. The switch default setting for egress queues scheduling is Weighted Round Robin (WRR).

You may complete the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes via the Class of Service settings. Depending on the platform, these choices may include strict priority for the queue used for iSCSI traffic. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic may get starved. In WRR the queue to which the flow is assigned to can be set to get the required percentage.

Format: iscsi cos {vpt | dscp} [remark]
Mode: Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpt/dscp</td>
<td>The VLAN Priority Tag or DSCP to assign iSCSI session packets.</td>
</tr>
<tr>
<td>remark</td>
<td>Mark the iSCSI frames with the configured VPT/DSCP when egressing the switch.</td>
</tr>
</tbody>
</table>

**Example:** The following example sets the quality of service profile that will be applied to iSCSI flows.

((switch)(config)#iscsi cos vpt 5 remark

7.12.2.1 no iscsi cos

Use the no form of the command to return to the default.

Format: no iscsi cos
Mode: Global Config

7.12.3 iscsi enable

This command globally enables iSCSI awareness.

Default: disabled
Format: iscsi enable
Mode: Global Config

**Example:** The following example enables iSCSI awareness.

((switch)(config)#iscsi enable
7.12.3.1  no iscsi enable
This command disables iSCSI awareness. When you use the no iscsi enable command, iSCSI resources will be released.

Format  no iscsi enable
Mode    Global Config

7.12.4  iscsi target port
This command configures an iSCSI target port and, optionally, a target system's IP address and IQN name. When working with private iSCSI ports (not IANA-assigned ports 3260/860), it is recommended to specify the target IP address as well, so that the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, and the destination IP is the target's IP address. This way the CPU will not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these un-reserved ports).

When a port is already defined and not bound to an IP address, and you want to bind it to an IP address, you should first remove it by using the no form of the command and then add it again, this time together with the relevant IP address.

Target names are only for display when using the show iscsi command. These names are not used to match with the iSCSI session information acquired by snooping.

A maximum of 16 TCP ports can be configured either bound to IP or not.

Default  iSCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target.

Format  iscsi target port tcp-port-1 [tcp-port-2...tcp-port-16] [address ip-address] [name targetname]
Mode    Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp-port-n</td>
<td>TCP port number or list of TCP port numbers on which the iSCSI target listens to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the iSCSI target. When the no form of this command is used, and the tcp port to be deleted is one bound to a specific IP address, the address field must be present.</td>
</tr>
<tr>
<td>targetname</td>
<td>iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSNS or from sendTargets response. The initiator must present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection.</td>
</tr>
</tbody>
</table>

Example: The following example configures TCP Port 49154 to target IP address 172.16.1.20.
(switch)(config)#iscsi target port 49154 address 172.16.1.20
7.12.4.1  no iscsi target port

Use the no form of the command to delete an iSCSI target port, address, and name.

7.12.5  show iscsi

This command displays the iSCSI settings.

**Format**

```
show iscsi
```

**Mode**

Privileged EXEC

**Example:** The following are examples of the commands used for iSCSI.

**Example #1: Show iSCSI (Default Configuration)**

```
(switch)#show iscsi
iSCSI disabled
iSCSI vpt is 5, remark
Session aging time: 10 min
Maximum number of sessions is 192

-----------------------------
iSCSI Targets and TCP ports:
-----------------------------
TCP Port  Target IP Address  Name
860       Not Configured     Not Configured
3260      Not Configured     Not Configured
```

**Example #2: Enable iSCSI.**

```
(switch)#configure
(switch)(config)#iscsi enable
```

**Example #3: Show iSCSI (After Enable)**

The following configuration detects iSCSI sessions and connections established using TCP ports 3260 or 860. Packets sent on detected iSCSI TCP connections are assigned to traffic class 2 (see the CoS configuration shown below). Since remark is enabled, the packets are marked with IEEE 802.1p priority to 5 before transmission.

```
(switch)#show iscsi
iscsi enabled
iSCSI vpt is 5, remark
Session aging time: 10 min
Maximum number of sessions is 192

-----------------------------
iSCSI Targets and TCP ports:
-----------------------------
TCP Port  Target IP Address  Name
860       Not Configured     Not Configured
3260      Not Configured     Not Configured

(switch)#show classofservice dot1p-mapping
User Priority  Traffic Class
--------  ----------
0           1
1           0
2           0
3           1
4           2
5           2
6           3
6           3
```
7.12.6 show iscsi sessions

This command displays the iSCSI sessions.

**Default**
If not specified, sessions are displayed in short mode (not detailed).

**Format**
show iscsi sessions [detailed]

**Mode**
Privileged EXEC

**Example:** The following example displays the iSCSI sessions.

```
(switch) # show iscsi sessions
---------------------------------------------
ISID: 11
ISID: 222
---------------------------------------------
  storage.tape:sys1.xyz
Session 3:
Session 4:
---------------------------------------------
```

```
(switch)# show iscsi sessions detailed
---------------------------------------------
Session 1:
  Time started: 17-Jul-2008 10:04:50
  Time for aging out: 10 min
  ISID: 11
  Initiator Initiator Target Target
  IP address TCP port IP address IP port
  172.16.1.3 49154 172.16.1.20 30001
  172.16.1.4 49155 172.16.1.21 30001
  172.16.1.5 49156 172.16.1.22 30001
---------------------------------------------
Session 2:
  Time started: 17-Aug-2008 21:04:50
  Time for aging out: 2 min
  ISID: 22
  Initiator Initiator Target Target
  IP address TCP port IP address IP port
  172.16.1.30 49200 172.16.1.20 30001
  172.16.1.30 49201 172.16.1.21 30001
```
8/ IP Multicast Commands

This chapter describes the IP Multicast commands available in the FASTPATH CLI.

The IP Multicast Commands chapter contains the following sections:

- “Multicast Commands” on page 803
- “DVMRP Commands” on page 812
- “PIM Commands” on page 816
- “Internet Group Message Protocol Commands” on page 830
- “IGMP Proxy Commands” on page 837

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.

8.1 Multicast Commands

This section describes the commands you use to configure IP Multicast and to view IP Multicast settings and statistics.

8.1.1 ip mcast boundary

This command adds an administrative scope multicast boundary specified by `groupipaddr` and `mask` for which this multicast administrative boundary is applicable. `groupipaddr` is a group IP address and `mask` is a group IP mask. This command can be used to configure a single interface or a range of interfaces.

Format: `ip mcast boundary groupipaddr mask`
Mode: Interface Config

8.1.1.1 no ip mcast boundary

This command deletes an administrative scope multicast boundary specified by `groupipaddr` and `mask` for which this multicast administrative boundary is applicable. `groupipaddr` is a group IP address and `mask` is a group IP mask.

Format: `no ip mcast boundary groupipaddr mask`
Mode: Interface Config

8.1.2 ip mroute

This command configures an IPv4 Multicast Static Route for a source.

Default: No MRoute is configured on the system.

Format: `ip mroute src-ip-addr src-mask rpf-addr preference`
Mode: Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src-ip-addr</td>
<td>The IP address of the multicast source network.</td>
</tr>
<tr>
<td>src-mask</td>
<td>The IP mask of the multicast data source.</td>
</tr>
<tr>
<td>rpf-ip-addr</td>
<td>The IP address of the RPF next-hop router toward the source.</td>
</tr>
<tr>
<td>preference</td>
<td>The administrative distance for this Static MRoute, that is, the preference value. The range is 1 to 255.</td>
</tr>
</tbody>
</table>
8.1.2.1  **no ip mroute**  
This command removes the configured IPv4 Multicast Static Route.

**Format**  
no ip mroute src-ip-addr  
**Mode**  
Global Config

8.1.3  **ip multicast**  
This command sets the administrative mode of the IP multicast forwarder in the router to active. This command also enables the administrative mode of IPv6 multicast routing.

**Default**  
disabled  
**Format**  
ip multicast  
**Mode**  
Global Config

8.1.3.1  **no ip multicast**  
This command sets the administrative mode of the IP multicast forwarder in the router to inactive.

**Format**  
o ip multicast  
**Mode**  
Global Config

8.1.4  **ip multicast ttl-threshold**  
This command is specific to IPv4. Use this command to apply the given Time-to-Live threshold value to a routing interface or range of interfaces. The **ttl**-**threshold** is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. This command sets the Time-to-Live threshold value such that any data packets forwarded over the interface having TTL value above the configured value are dropped. The value for **ttl**-**threshold** ranges from 0 to 255.

**Default**  
1  
**Format**  
ip multicast ttl-threshold ttlvalue  
**Mode**  
Interface Config

8.1.4.1  **no ip multicast ttl-threshold**  
This command applies the default **ttl**-**threshold** to a routing interface. The **ttl**-**threshold** is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

**Format**  
o ip multicast ttl-threshold  
**Mode**  
Interface Config

8.1.5  **show ip mcast**  
This command displays the system-wide multicast information.

**Format**  
show ip mcast  
**Modes**  
• Privileged EXEC  
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>The administrative status of multicast. Possible values are enabled or disabled.</td>
</tr>
</tbody>
</table>
8.1.6 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Format  show ip mcast boundary {slot/port|vlan 1-4093|all}
Modes  
  • Privileged EXEC
  • User EXEC

8.1.7 show ip mcast interface

This command displays the multicast information for the specified interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Format  show ip mcast interface {slot/port|vlan 1-4093}
Modes  
  • Privileged EXEC
  • User EXEC

8.1.8 show ip mroute

This command displays a summary or all the details of the multicast table.

This command replaces the show ip mcast mroute command.

Format  show ip mroute {detail | summary | group group-address | source source-address}
Modes  
  • Privileged EXEC
  • User EXEC
If you use the `detail`, `group`, or `source` parameters in PIM Sparse mode, the command displays the following fields:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Flags         | • F: Register flag. Indicates that the source connected router is sending registers to RP. This flag can be seen only on Designated Router connected to source.  
• T: SPT-bit set. Indicates that packets have been received on the shortest path source tree.  
• R: RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This flag typically indicates a prune state along the shared tree for a particular source.  |
| Outgoing interface flags | • C: Connected. A member of the multicast group is directly connected to the interface.  
• J: Received PIM (*,G) Join on this interface.  |
| Timers:Uptime/Expires | • Uptime: Indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table.  
• Expires: Indicates per interface how long (in seconds) until the entry will be removed from the IP multicast routing table  |
| Counters | • Joins: Indicates the number of (*,G) or (S,G) joins received for the given entry.  
• Prunes: Indicates the number of (*,G) or (S,G) prunes received for the given entry.  
• Registers: Indicates the number of register messages received for the given (S,G) entry.  
• Register Stops: Indicates the number of register stop messages received for the given (S,G) entry.  |
| RPF Address | IP address of the upstream router to the source.  |
| Outgoing interface list | List of outgoing Interfaces.  |
| Protocol | The current operating multicast routing protocol.  |
| RP | Address of the RP router.  |
| Incoming interface | Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.  |

If you use the `detail` parameter in any mode other than PIM sparse mode, the command displays the following fields:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The time of expiry of this entry in seconds.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time elapsed since the entry was created in seconds.</td>
</tr>
<tr>
<td>RPF Neighbor</td>
<td>The IP address of the RPF neighbor.</td>
</tr>
<tr>
<td>Flags</td>
<td>The flags associated with this entry.</td>
</tr>
</tbody>
</table>

If you use the `summary` parameter in PIM Sparse mode, the command displays the following fields:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Source address of the multicast route entry.</td>
</tr>
<tr>
<td>Group IP</td>
<td>Group address of the multicast route entry.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The current operating multicast routing protocol.</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.</td>
</tr>
<tr>
<td>Outgoing Interface List</td>
<td>List of outgoing Interfaces.</td>
</tr>
</tbody>
</table>
If you use the summary parameter, the command displays the following fields:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The multicast routing protocol by which the entry was created.</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>The interface on which the packet for the source/group arrives.</td>
</tr>
<tr>
<td>Outgoing Interface List</td>
<td>The list of outgoing interfaces on which the packet is forwarded.</td>
</tr>
</tbody>
</table>

**Example:** This example shows the output for the summary parameter in PIM Sparse mode.

(FASTPATH Routing) #show ip mroute summary

```plaintext
Multicast route table summary

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Group IP</th>
<th>Protocol</th>
<th>Incoming Interface</th>
<th>Outgoing Interface List</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.1</td>
<td>225.1.1.1</td>
<td>PIMSM</td>
<td>Vl10</td>
<td>Vl20, Vl30</td>
</tr>
</tbody>
</table>
```

**Example:** This example shows the output for the detail parameter in PIM Sparse mode.

**IP Multicast Routing Table**

Flags: C - Connected, J - Received Pim (*,G) Join, R - RP-bit set, F - Register flag, T - SPT-bit set

Timers: Uptime/Expires Protocol: PIMSM

( *,225.6.6.6) 00:00:41/000 RP: 1.1.1.1
Joins/Prunes: 0/0
Incoming interface: RPF nbr: 0.0.0.0
Outgoing interface list: 4/1 00:00:41/218 Joins: 0 Flags: C

( *,225.7.7.7) 00:00:36/000 RP: 1.1.1.1
Joins/Prunes: 0/0
Incoming interface: RPF nbr: 0.0.0.0
Outgoing interface list: 4/1 00:00:36/224 Joins: 0 Flags: C

(3.3.3.11,225.6.6.6) 00:00:51/158 Flags: T
Joins/Prunes: 0/0 Reg/Reg-stop: 0/0
Incoming interface: 4/2 RPF nbr: 3.3.3.11
Outgoing interface list: 4/1 00:00:41/000 Joins: 0

(3.3.3.11,225.7.7.7) 00:17:42/201 Flags: T
Joins/Prunes: 0/0 Reg/Reg-stop: 0/0
Incoming interface: 4/2 RPF nbr: 3.3.3.11
Outgoing interface list: 4/1 00:00:36/000 Joins: 0
**Example:** This example shows the output for the detail parameter in PIM Dense mode when a multicast routing protocol other than PIMSM is enabled.

```
(FASTPATH Routing) (Config)#show ip mroute detail
```

**Example:** This example shows the output for the group parameter in PIM Sparse mode.

```
(U16)# show ip mroute group 229.10.0.1
```

---

**Example:** This example shows the output for the detail parameter in PIM Sparse mode.

```
# show ipv6 mroute detail
```

Example: This example shows IPv6 output for the detail parameter in PIM Sparse mode.

```
# show ipv6 mroute detail
```

**Example:** This example shows output for the group parameter in PIM Sparse mode.

```
(U16)# show ip mroute group 229.10.0.1
```

---

**Example:** This example shows the output for the detail parameter in PIM Dense mode when a multicast routing protocol other than PIMSM is enabled.

```
(FASTPATH Routing) (Config)#show ip mroute detail
```

**Example:** This example shows IPv6 output for the detail parameter in PIM Sparse mode.

```
# show ipv6 mroute detail
```

Example: This example shows the output for the group parameter in PIM Sparse mode.

```
(U16)# show ip mroute group 229.10.0.1
```
Exercise: The following example shows output for the source parameter in PIM Sparse mode.

```
(U16)# show ip mroute source 192.0.2.20
IP Multicast Routing Table

Flags: C - Connected, J - Received PIM (*,G) Join,
R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime(HH:MM:SS)/Expiry(SSS)
Protocol: PIMSM

(192.0.2.20, 229.10.0.1), 00:04:35/177, Flags: T
Joins/Prunes:20/1, Reg/Reg-Stop:100/0
Incoming interface: VLAN 2, RPF Address: 0.0.0.0
Outgoing interface list:
  VLAN 5 00:03:25/0 Joins:20
  VLAN 6 00:00:10/0 Joins:5

8.1.9 show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given groupipaddr.

Format
show ip mcast mroute group groupipaddr {detail | summary}

Modes
• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The multicast routing protocol by which this entry was created.</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>The interface on which the packet for this group arrives.</td>
</tr>
<tr>
<td>Outgoing Interface List</td>
<td>The list of outgoing interfaces on which this packet is forwarded.</td>
</tr>
</tbody>
</table>

8.1.10 show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given source IP address or source IP address and group IP address pair.

Format
show ip mcast mroute source sourceipaddr {summary | groupipaddr}

Modes
• Privileged EXEC
• User EXEC
If you use the `groupipaddr` parameter, the command displays the following column headings in the output table:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The time of expiry of this entry in seconds.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time elapsed since the entry was created in seconds.</td>
</tr>
<tr>
<td>RPF Neighbor</td>
<td>The IP address of the RPF neighbor.</td>
</tr>
<tr>
<td>Flags</td>
<td>The flags associated with this entry.</td>
</tr>
</tbody>
</table>

If you use the `summary` parameter, the command displays the following column headings in the output table:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The multicast routing protocol by which this entry was created.</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>The interface on which the packet for this source arrives.</td>
</tr>
<tr>
<td>Outgoing Interface List</td>
<td>The list of outgoing interfaces on which this packet is forwarded.</td>
</tr>
</tbody>
</table>

### 8.1.11 show ip mcast mroute static

Use the `show ip mcast mroute static` command in Privileged EXEC or User EXEC mode to display all the static routes configured in the static mcast table, if it is specified, or display the static route associated with the particular `sourceipaddr`.

**Format**

```
show ip mcast mroute static [sourceipaddr]
```

**Modes**

- Privileged EXEC
- User EXEC

**Parameter**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>IP address of the multicast source network.</td>
</tr>
<tr>
<td>Source Mask</td>
<td>The subnetwork mask pertaining to the sourceIP.</td>
</tr>
<tr>
<td>RPF Address</td>
<td>The IP address of the RPF next-hop router toward the source.</td>
</tr>
<tr>
<td>Preference</td>
<td>The administrative distance for this Static MRoute.</td>
</tr>
</tbody>
</table>

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

```
console#show ip mcast mroute static
```

```
MULTICAST STATIC ROUTES
Source IP Source Mask RPF Address Preference
--------------- -------------- -------------- --------------
1.1.1.1 255.255.255.0 2.2.2.2 23
```
8.1.12 clear ip mroute
This command deletes all or the specified IP multicast route entries.

**NOTICE**
This command only clears dynamic mroute entries. It does not clear static mroutes.

**Format**
clear ip mroute {*|group-address[source-address]}

**Modes**
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Deletes all IPv4 entries from the IP multicast routing table.</td>
</tr>
<tr>
<td>group-address</td>
<td>IP address of the multicast group.</td>
</tr>
<tr>
<td>source-address</td>
<td>The IP address of a multicast source that is sending multicast traffic to the group.</td>
</tr>
</tbody>
</table>

**Example:**
The following deletes all entries from the IP multicast routing table:
(Broadcom FASTPATH Routing) # clear ip mroute *

**Example:**
The following deletes all entries from the IP multicast routing table that match the given multicast group address (224.1.2.1), irrespective of which source is sending for this group:
(Broadcom FASTPATH Routing) # clear ip mroute 224.1.2.1

**Example:**
The following deletes all entries from the IP multicast routing table that match the given multicast group address (224.1.2.1) and the multicast source address (192.168.10.10):
(Broadcom FASTPATH Routing) # clear ip mroute 224.1.2.1 192.168.10.10

8.1.13 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 behavior that such packets are dropped (argument 'none'). The flooding mode is set per port. It can be applied to either individual physical ports or to a port-channel.

**Format**
multicast flood {default | none}

**Mode**
Interface Config

8.1.14 show port multicast
This command displays the port based multicast handling. The commands displays for a specified interface or all interfaces the multicast flooding settings. The displayed fields are
- the interface
- the multicast flooding, indicating whether a packet with unregistered multicast address should be flooded or not (yes/no).

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

**Mode**
Privileged Exec
8.2 DVMRP Commands
This section describes the Distance Vector Multicast Routing Protocol (DVMRP) commands.

8.2.1 ip dvmrp
This command sets administrative mode of DVMRP in the router to active.

| Default   | disabled     |
| Format    | ip dvmrp     |
| Mode      | Global Config|

8.2.1.1 no ip dvmrp
This command sets administrative mode of DVMRP in the router to inactive.

| Format    | no ip dvmrp |
| Mode      | Global Config|

8.2.2 ip dvmrp metric
This command configures the metric for an interface or range of interfaces. This value is used in the DVMRP messages as the cost to reach this network. This field has a range of 1 to 31.

| Default   | 1           |
| Format    | ip dvmrp metric metric |
| Mode      | Interface Config|

8.2.2.1 no ip dvmrp metric
This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

| Format    | no ip dvmrp metric |
| Mode      | Interface Config|

8.2.3 ip dvmrp trapflags
This command enables the DVMRP trap mode.

| Default   | disabled     |
| Format    | ip dvmrp trapflags |
| Mode      | Global Config |
8.2.3.1 no ip dvmrp trapflags
This command disables the DVMRP trap mode.

Format  no ip dvmrp trapflags
Mode    Global Config

8.2.4 ip dvmrp
This command sets the administrative mode of DVMRP on an interface or range of interfaces to active.

Default  disabled
Format    ip dvmrp
Mode      Interface Config

8.2.4.1 no ip dvmrp
This command sets the administrative mode of DVMRP on an interface to inactive.

Format    no ip dvmrp
Mode      Interface Config

8.2.5 show ip dvmrp
This command displays the system-wide information for DVMRP.

Format    show ip dvmrp
Modes     • Privileged EXEC
          • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Mode</td>
<td>Indicates whether DVMRP is enabled or disabled.</td>
</tr>
<tr>
<td>Version String</td>
<td>The version of DVMRP being used.</td>
</tr>
<tr>
<td>Number of Routes</td>
<td>The number of routes in the DVMRP routing table.</td>
</tr>
<tr>
<td>Reachable Routes</td>
<td>The number of entries in the routing table with non-infinite metrics.</td>
</tr>
</tbody>
</table>

The following fields are displayed for each interface.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>The mode of this interface. Possible values are Enabled and Disabled.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.</td>
</tr>
</tbody>
</table>
8.2.6  show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

**Format**

```
show ip dvmrp interface {slot/port|vlan [1-4093]}
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Mode</td>
<td>Indicates whether DVMRP is enabled or disabled on the specified interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric of this interface. This is a configured value.</td>
</tr>
<tr>
<td>Local Address</td>
<td>The IP address of the interface.</td>
</tr>
</tbody>
</table>

The following field is displayed only when DVMRP is operational on the interface.

**Term**

**Definition**

The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

The following fields are displayed only if DVMRP is enabled on this interface.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Bad Packets</td>
<td>The number of invalid packets received.</td>
</tr>
<tr>
<td>Received Bad Routes</td>
<td>The number of invalid routes received.</td>
</tr>
<tr>
<td>Sent Routes</td>
<td>The number of routes that have been sent on this interface.</td>
</tr>
</tbody>
</table>

8.2.7  show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

**Format**

```
show ip dvmrp neighbor
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IfIndex</td>
<td>The value of the interface used to reach the neighbor.</td>
</tr>
<tr>
<td>Nbr IP Addr</td>
<td>The IP address of the DVMRP neighbor for which this entry contains information.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time since this neighboring router was learned.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.</td>
</tr>
<tr>
<td>Generation ID</td>
<td>The Generation ID value for the neighbor.</td>
</tr>
<tr>
<td>Major Version</td>
<td>The major version of DVMRP protocol of neighbor.</td>
</tr>
<tr>
<td>Minor Version</td>
<td>The minor version of DVMRP protocol of neighbor.</td>
</tr>
<tr>
<td>Capabilities</td>
<td>The capabilities of neighbor.</td>
</tr>
<tr>
<td>Received Routes</td>
<td>The number of routes received from the neighbor.</td>
</tr>
<tr>
<td>Rcvd Bad Pkts</td>
<td>The number of invalid packets received from this neighbor.</td>
</tr>
</tbody>
</table>
### 8.2.8 show ip dvmrp nexthop
This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip dvmrp nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modes</td>
<td>• Privileged EXEC</td>
</tr>
<tr>
<td></td>
<td>• User EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvd Bad Routes</td>
<td>The number of correct packets received with invalid routes.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The sources for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>Source Mask</td>
<td>The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.</td>
</tr>
<tr>
<td>Next Hop Interface</td>
<td>The interface in <em>slot/port</em> format for the outgoing interface for this next hop.</td>
</tr>
<tr>
<td>Type</td>
<td>The network is a LEAF or a BRANCH.</td>
</tr>
</tbody>
</table>

### 8.2.9 show ip dvmrp prune
This command displays the table listing the router’s upstream prune information.

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip dvmrp prune</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modes</td>
<td>• Privileged EXEC</td>
</tr>
<tr>
<td></td>
<td>• User EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group IP</td>
<td>The multicast Address that is pruned.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The IP address of the source that has pruned.</td>
</tr>
<tr>
<td>Source Mask</td>
<td>The network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.</td>
</tr>
<tr>
<td>Expiry Time (secs)</td>
<td>The expiry time in seconds. This is the time remaining for this prune to age out.</td>
</tr>
</tbody>
</table>

### 8.2.10 show ip dvmrp route
This command displays the multicast routing information for DVMRP.

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip dvmrp route</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modes</td>
<td>• Privileged EXEC</td>
</tr>
<tr>
<td></td>
<td>• User EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>The multicast address of the source group.</td>
</tr>
<tr>
<td>Source Mask</td>
<td>The IP Mask for the source group.</td>
</tr>
<tr>
<td>Upstream Neighbor</td>
<td>The IP address of the neighbor which is the source for the packets for a specified multicast address.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface used to receive the packets sent by the sources.</td>
</tr>
<tr>
<td>Metric</td>
<td>The distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.</td>
</tr>
</tbody>
</table>
8.3 PIM Commands

This section describes the commands you use to configure Protocol Independent Multicast – Dense Mode (PIM-DM) and Protocol Independent Multicast – Sparse Mode (PIM-SM). PIM-DM and PIM-SM are multicast routing protocols that provide scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. Only one PIM mode can be operational at a time.

8.3.1 ip pim dense

This command administratively enables the PIM Dense mode across the router.

**Default** disabled

**Format** ip pim dense

**Mode** Global Config

**Example:** The following shows an example of the command.

(FASTPATH) (Config) #ip pim dense

8.3.1.1 no ip pim dense

This command administratively disables the PIM Dense mode across the router.

**Format** no ip pim dense

**Mode** Global Config

8.3.2 ip pim sparse

This command administratively enables the PIM Sparse mode across the router.

**Default** disabled

**Format** ip pim sparse

**Mode** Global Config

**Example:** The following shows an example of the command.

(FASTPATH) (Config) #ip pim sparse
8.3.2.1  **no ip pim sparse**  
This command administratively disables the PIM Sparse mode across the router.

**Format**  
no ip pim sparse  
**Mode**  
Global Config

8.3.3  **ip pim**  
Use this command to administratively enable PIM on the specified interface.

**Default**  
disabled  
**Format**  
ip pim  
**Mode**  
Interface Config

**Example:** The following shows example CLI display output for the command.
(FASTPATH) (Interface 0/1) #ip pim

8.3.3.1  **no ip pim**  
Use this command to disable PIM on the specified interface.

**Format**  
no ip pim  
**Mode**  
Interface Config

8.3.4  **ip pim hello-interval**  
This command configures the transmission frequency of PIM hello messages the specified interface. This field has a range of 0 to 18000 seconds.

**Default**  
30  
**Format**  
 ip pim hello-interval seconds  
**Mode**  
Interface Config

**Example:** The following shows an example of the command.
(FASTPATH) (Interface 0/1) #ip pim hello-interval 50
8.3.4.1  no ip pim hello-interval
This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format  no ip pim hello-interval
Mode    Interface Config

8.3.5  ip pim bsr-border
Use this command to prevent bootstrap router (BSR) messages from being sent or received on the specified interface.

Example: The following shows an example of the command.
(FASTPATH) (Interface 8/1) #ip pim bsr-border

8.3.5.1  no ip pim bsr-border
Use this command to disable the specified interface from being the BSR border.

Format  no ip pim bsr-border
Mode    Interface Config

8.3.6  ip pim bsr-candidate
This command is used to configure the router to announce its candidacy as a bootstrap router (BSR). The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Notice: This command takes effect only when Sparse mode is enabled in the Global mode.

Default  disabled
Format  ip pim bsr-candidate interface {slot/port|vlan 1-4093} hash-mask-length [bsr-priority] [interval interval]
Mode    Global Config

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Interface number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with PIM.</td>
</tr>
<tr>
<td>hash-mask-length</td>
<td>Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.</td>
</tr>
</tbody>
</table>
### Example:
The following shows examples of the command.

```plaintext
(FASTPATH) (Config) #ip pim bsr-candidate interface 0/1 32 5
(FASTPATH) (Config) #ip pim bsr-candidate interface 0/1 32 5 interval 100
```

#### 8.3.6.1 no ip pim bsr-candidate

Use this command to remove the configured PIM Candidate BSR router.

**Format**
```
no ip pim bsr-candidate interface {slot/port|vlan 1-4093}
```

**Mode**
Global Config

#### 8.3.7 ip pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR).

**Notice:** This command takes effect only when Sparse mode is enabled in the Global mode.

**Default**
1

**Format**
```
ip pim dr-priority 0-2147483647
```

**Mode**
Interface Config

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

```
(FASTPATH) (Interface 0/1) #ip pim dr-priority 10
```
8.3.7.1  no ip pim dr-priority
Use this command to return the DR Priority on the specified interface to its default value.

**Format**  
no ip pim dr-priority

**Mode**  
Interface Config

8.3.8  ip pim join-prune-interval
Use this command to configure the frequency of PIM Join/Prune messages on a specified interface. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

---

**NOTICE**

This command takes effect only when is configured as the PIM mode.

**Default**  
60

**Format**  
ip pim join-prune-interval 0-18000

**Mode**  
Interface Config

---

**Example:** The following shows examples of the command.
(FASTPATH) (Interface 0/1) #ip pim join-prune-interval 90

8.3.8.1  no ip pim join-prune-interval
Use this command to set the join/prune interval on the specified interface to the default value.

**Format**  
no ip pim join-prune-interval

**Mode**  
Interface Config

8.3.9  ip pim rp-address
This command defines the address of a PIM Rendezvous point (RP) for a specific multicast group range.

---

**NOTICE**

This command takes effect only when PIM-SM is configured as the PIM mode.

**Default**  
0

**Format**  
ip pim rp-address rp-address group-address group-mask [override]

**Mode**  
Global Config

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp-address</td>
<td>The IP address of the RP.</td>
</tr>
<tr>
<td>group-address</td>
<td>The group address supported by the RP.</td>
</tr>
<tr>
<td>group-mask</td>
<td>The group mask for the group address.</td>
</tr>
<tr>
<td>override</td>
<td>[Optional] Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.</td>
</tr>
</tbody>
</table>
Example: The following shows an example of the command.
(FASTPATH) (Config) #ip pim rp-address 192.168.10.1 224.1.2.0 255.255.255.0

8.3.9.1 no ip pim rp-address
Use this command to remove the address of the configured PIM Rendezvous point (RP) for the specified multicast group range.

Format no ip pim rp-address rp-address group-address group-mask [override]
Mode Global Config

8.3.10 ip pim rp-candidate
Use this command to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR) for a specific multicast group range. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

Example: The following shows examples of the command.
(FASTPATH) (Config) #ip pim rp-candidate interface 0/1 224.1.2.0 255.255.255.0
(FASTPATH) (Config) #ip pim rp-candidate interface 0/1 224.1.2.0 255.255.255.0 interval 200

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>The IP address associated with this interface type and number is advertised as a candidate RP address. This interface must be enabled with PIM.</td>
</tr>
<tr>
<td>group-address</td>
<td>The multicast group address that is advertised in association with the RP address.</td>
</tr>
<tr>
<td>group-mask</td>
<td>The multicast group prefix that is advertised in association with the RP address.</td>
</tr>
<tr>
<td>interval</td>
<td>[Optional] Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.</td>
</tr>
</tbody>
</table>
8.3.10.1  no ip pim rp-candidate
Use this command to remove the configured PIM candidate Rendezvous point (RP) for a specific multicast group range.

**Format**

no ip pim rp-candidate interface \{slot/port|vlan 1-4093\} group-address group-mask

**Mode**

Global Config

8.3.11  ip pim ssm
Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

---

**NOTICE**

This command takes effect only when PIM-SM is configured as the PIM mode.

**Default**

disabled

**Format**

ip pim ssm \{default | group-address group-mask\}

**Mode**

Global Config

---

**Parameter** | **Description**
--- | ---
default-range | Defines the SSM range access list to 232/8.

**Example:** The following shows an example of the command.

(FASTPATH) (Config) #ip pim ssm default

(FASTPATH) (Config) #ip pim ssm 232.1.2.0 255.255.255.0

8.3.11.1  no ip pim ssm
Use this command to remove the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

**Format**

no ip pim ssm \{default | group-address group-mask\}

**Mode**

Global Config

8.3.12  ip pim-trapflags
This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode (DM).

**Default**

disabled

**Format**

ip pim-trapflags

**Mode**

Global Config
8.3.12.1 no ip pim-trapflags
This command sets the PIM trap mode to the default.

**Format**
no ip pim-trapflags

**Mode**
Global Config

8.3.13 ip pim spt-threshold
Use this command to configure the Data Threshold rate for the last-hop router to switch to the shortest path on the router. The rate is specified in Kilobits per second. The possible values are 0 to 2000.

---

**NOTICE**
This command takes effect only when PIM-SM is configured as the PIM mode.

**Default**
0

**Format**
ip pim spt-threshold 0-2000

**Modes**
Global Config

**Example:** The following shows an example of the command.

```plaintext
(FASTPATH) (Config) #ip pim spt-threshold 100
```

8.3.13.1 no ip pim spt-threshold
This command is used to set the data threshold rate for the RP router to the default value.

**Format**
no ip pim-spt-threshold

**Mode**
Global Config

8.3.14 show ip mfc
This command displays mroute entries in the multicast forwarding (MFC) database.

**Format**
show ip mfc

**Modes**
- Privileged EXEC
- User EXEC

---

<table>
<thead>
<tr>
<th>Terms</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFC IPv4 Mode</td>
<td>Enabled when IPv4 Multicast routing is operational.</td>
</tr>
<tr>
<td>MFC IPv6 Mode</td>
<td>Enabled when IPv6 Multicast routing is operational.</td>
</tr>
<tr>
<td>MFC Entry Count</td>
<td>The number of entries present in MFC.</td>
</tr>
<tr>
<td>Current multicast IPv4 Protocol</td>
<td>The current operating IPv4 multicast routing protocol.</td>
</tr>
<tr>
<td>Current multicast IPv6 Protocol</td>
<td>The current operating multicast IPv6 routing protocol.</td>
</tr>
<tr>
<td>Total Software Forwarded packets</td>
<td>Total Number of multicast packets forwarded in software.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address of the multicast route entry.</td>
</tr>
<tr>
<td>Group Address</td>
<td>Group address of the multicast route entry.</td>
</tr>
<tr>
<td>Packets Forwarded in Software for this entry</td>
<td>Number of multicast packets that are forwarded in software for a specific multicast route entry.</td>
</tr>
</tbody>
</table>
Example:
(FASTPATH Routing) (Config)#show ip mfc

MFC IPv4 Mode.......................... Enabled
MFC IPv6 Mode.......................... Disabled
MFC Entry Count........................ 1
Current multicast IPv4 protocol.............. PIMSM
Current multicast IPv6 protocol.............. No protocol enabled.
Total software forwarded packets .......... 0

Source address: 192.168.10.5
Group address: 225.1.1.1
Packets forwarded in software for this entry: 0

Protocol: PIM-SM
Expiry Time (secs): 206
Up Time (secs): 4
Incoming interface: 0/10
Outgoing interface list: None

8.3.15 show ip pim

This command displays the system-wide information for PIM-DM or PIM-SM.

Format
show ip pim

Modes
• Privileged EXEC
• User EXEC

If the PIM mode is PIM-DM (dense), some of the fields in the following table do not display in the command output because they are applicable only to PIM-SM.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM Mode</td>
<td>Indicates the configured mode of the PIM protocol as dense (PIM-DM) or sparse (PIM-SM)</td>
</tr>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>Indicates whether PIM is enabled or disabled on this interface.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The current state of PIM on this interface: Operational or Non-Operational.</td>
</tr>
</tbody>
</table>

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

Example #1: PIM Mode - Dense
(FASTPATH) #show ip pim

PIM Mode Dense

Interface Interface-Mode Operational Status
-------- ----------- ---------------
0/1  Enabled   Operational
0/3  Disabled  Non-Operational

Example #2: PIM Mode - Sparse
(FASTPATH) #show ip pim
Example #3: PIM Mode - None

(FASTPATH) #show ip pim

PIM Mode  None

None of the routing interfaces are enabled for PIM.

8.3.16  show ip pim ssm

This command displays the configured source specific IP multicast addresses. If no SSM Group range is configured, this command output is:

No SSM address range is configured.

**Format**  show ip pim ssm

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The IP multicast address of the SSM group.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>The network prefix length.</td>
</tr>
</tbody>
</table>

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

(FASTPATH) #show ip pim ssm

Group Address/Prefix Length

---

232.0.0.0/8

If no SSM Group range is configured, this command displays the following message:

No SSM address range is configured.

8.3.17  show ip pim interface

This command displays the PIM interface status parameters. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format. If no interface is specified, the command displays the status parameters of all PIM-enabled interfaces.

**Format**  show ip pim interface [slot/port|vlan 1-4093]}

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port The interface number.</td>
</tr>
<tr>
<td>Mode</td>
<td>Indicates the active PIM mode enabled on the interface is dense or sparse.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(FASTPATH) #show ip pim interface

Interface.........................................0/1
  Mode............................................Sparse
  Hello Interval (secs)...........................30
  Join Prune Interval (secs)......................60
  DR Priority.....................................1
  BSR Border......................................Disabled
  Neighbor Count..................................1
  Designated Router...............................192.168.10.1

Interface.........................................0/2
  Mode............................................Sparse
  Hello Interval (secs)...........................30
  Join Prune Interval (secs)......................60
  DR Priority.....................................1
  BSR Border......................................Disabled
  Neighbor Count..................................1
  Designated Router...............................192.168.10.1

If none of the interfaces are enabled for PIM, the following message is displayed:
None of the routing interfaces are enabled for PIM.

8.3.18 show ip pim neighbor

This command displays PIM neighbors discovered by PIMv2 Hello messages. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format. If the interface number is not specified, the command displays the status parameters of all PIM-enabled interfaces.

Format  show ip pim neighbor [{slot/port|vlan 1-4093}]

Modes
•  Privileged EXEC
•  User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Address</td>
<td>The IP address of the PIM neighbor on an interface.</td>
</tr>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time since this neighbor has become active on this interface.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Time remaining for the neighbor to expire.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>The DR Priority configured on this Interface (PIM-SM only).</td>
</tr>
</tbody>
</table>

  Note: DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

  Note: DR indicates that the neighbor is the PIM Designated Router in that subnet.
**Example:** The following shows example CLI display output for the command.

(FASTPATH) #show ip pim neighbor 0/1

<table>
<thead>
<tr>
<th>Neighbor Addr</th>
<th>Interface</th>
<th>Uptime (hh:mm:ss)</th>
<th>Expiry Time (hh:mm:ss)</th>
<th>DR Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.2</td>
<td>0/1</td>
<td>00:02:55</td>
<td>00:01:15</td>
<td>10 (DR)</td>
</tr>
</tbody>
</table>

(FASTPATH) #show ip pim neighbor

<table>
<thead>
<tr>
<th>Neighbor Addr</th>
<th>Interface</th>
<th>Uptime (hh:mm:ss)</th>
<th>Expiry Time (hh:mm:ss)</th>
<th>DR Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.2</td>
<td>0/1</td>
<td>00:02:55</td>
<td>00:01:15</td>
<td>10 (DR)</td>
</tr>
<tr>
<td>192.168.20.2</td>
<td>0/2</td>
<td>00:03:50</td>
<td>00:02:10</td>
<td>1</td>
</tr>
</tbody>
</table>

If no neighbors have been learned on any of the interfaces, the following message is displayed:

No neighbors exist on the router.

### 8.3.19 show ip pim bsr-router

This command displays the bootstrap router (BSR) information.

**Format**

`show ip pim bsr-router {candidate | elected}`

**Mode**

- Privileged EXEC
- User EXEC

---

**Parameter** | **Definition**
---|---
BSR Address | IP address of the BSR.
BSR Priority | Priority as configured in the `ip pim bsr-candidate` command.
BSR Hash Mask Length | Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the `ip pim bsr-candidate` command.
C-BSR Advertisement Interval | Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.
Next Bootstrap Message | Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

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

Example #1:

(FASTPATH) #show ip pim bsr-router elected

BSR Address........................................... 192.168.10.1
BSR Priority................................. 0
BSR Hash Mask Length......................... 30
Next Bootstrap message (hh:mm:ss)........... 00:00:24

Example #2:

(FASTPATH) #show ip pim bsr-router candidate

BSR Address........................................... 192.168.10.1
BSR Priority................................. 0
BSR Hash Mask Length......................... 30
C-BSR Advertisement Interval (secs)........... 0
Next Bootstrap message (hh:mm:ss)............. NA

If no configured or elected BSRs exist on the router, the following message is displayed:
No BSR's exist/learned on this router.

8.3.20 show ip pim rp-hash

This command displays the rendezvous point (RP) selected for the specified group address.

Format  show ip pim rp-hash group-address

Modes  
  • Privileged EXEC
  • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>The IP address of the RP for the group specified.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the mechanism (BSR or static) by which the RP was selected.</td>
</tr>
</tbody>
</table>

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

(FASTPATH) #show ip pim rp-hash 224.1.2.0

RP Address 192.168.10.1
Type Static

If no RP Group mapping exist on the router, the following message is displayed:
No RP-Group mappings exist/learned on this router.

8.3.21 show ip pim rp mapping

Use this command to display the mapping for the PIM group to the active Rendezvous points (RP) of which the router is aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address or to view group-to-candidate RP or group to Static RP mapping information.

Format  show ip pim rp mapping [{rp-address|candidate|static}]

Modes  
  • Privileged EXEC
  • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>The IP address of the RP for the group specified.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The IP address of the multicast group.</td>
</tr>
<tr>
<td>Group Mask</td>
<td>The subnet mask associated with the group.</td>
</tr>
<tr>
<td>Origin</td>
<td>Indicates the mechanism (BSR or static) by which the RP was selected.</td>
</tr>
<tr>
<td>C-RP Advertisement Interval</td>
<td>Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.</td>
</tr>
</tbody>
</table>

**Example:** The following show examples of CLI display output for the command.

Example #1:

(FASTPATH) #show ip pim rp mapping 192.168.10.1

RP Address 192.168.10.1
Group Address 224.1.2.1
Group Mask 255.255.255.0
Origin Static

Example #2:

(FASTPATH) #show ip pim rp mapping
RP Address 192.168.10.1
  Group Address 224.1.2.1
  Group Mask 255.255.255.0
  Origin Static
RP Address 192.168.20.1
  Group Address 229.2.0.0
  Group Mask 255.255.0.0
  Origin Static

Example #3:

(FASTPATH) # show ip pim rp mapping candidate

RP Address............................ 192.168.10.1
  Group Address.............................. 224.1.2.1
  Group Mask................................ 255.255.0.0
  Origin.................................... BSR
  C-RP Advertisement Interval (secs)........ 60
  Next Candidate RP Advertisement (hh:mm:ss). 00:00:15

If no RP Group mapping exist on the router, the following message is displayed:

No RP-Group mappings exist on this router.

8.3.22 show ip pim statistics

This command displays statistics for the received PIM control packets per interface. This command displays statistics only if PIM sparse mode is enabled.

Format show ip pim statistics

Modes
- Privileged EXEC
- User EXEC

The following information is displayed.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stat</td>
<td>RX: Packets received</td>
</tr>
<tr>
<td>Interface</td>
<td>The PIM-enabled routing interface</td>
</tr>
<tr>
<td>Hello</td>
<td>The number of PIM Hello messages</td>
</tr>
<tr>
<td>Register</td>
<td>The number of PIM Register messages</td>
</tr>
<tr>
<td>Reg-Stop</td>
<td>The number of PIM Register-stop messages</td>
</tr>
<tr>
<td>Join/Pru</td>
<td>The number of PIM Join/Prune messages</td>
</tr>
<tr>
<td>BSR</td>
<td>The number of PIM Boot Strap messages</td>
</tr>
<tr>
<td>Assert</td>
<td>The number of PIM Assert messages</td>
</tr>
<tr>
<td>CRP</td>
<td>The number of PIM Candidate RP Advertisement messages</td>
</tr>
</tbody>
</table>

Example:

Example 1:

(Routing) #show ip pim statistics

Interface Stat Hello Register Reg-Stop Join/Pru BSR Assert CRP
V110 Rx 0 0 0 0 0 0 0 0
  Tx 2 0 0 0 0 0 0
Invalid Packets Received - 0
V120 Rx 0 0 0 5 0 0 0 0
**Notice**

For ipv6 statistics use the key word ipv6.

### 8.4 Internet Group Message Protocol Commands

This section describes the commands you use to view and configure Internet Group Message Protocol (IGMP) settings.

#### 8.4.1 ip igmp

This command sets the administrative mode of IGMP in the system to active on an interface, range of interfaces, or on all interfaces.

- **Default**: disabled
- **Format**: `ip igmp`
- **Modes**:
  - Global Config
  - Interface Config

#### 8.4.1.1 no ip igmp

This command sets the administrative mode of IGMP in the system to inactive.

- **Format**: `no ip igmp`
- **Modes**:
  - Global Config
  - Interface Config
8.4.2 ip igmp header-validation
Use this command to enable header validation for IGMP messages.

Default: disabled
Format: ip igmp header-validation
Mode: Global Config

8.4.2.1 no ip igmp header-validation
This command disables header validation for IGMP messages.

Format: no ip igmp header-validation
Mode: Global Config

8.4.3 ip igmp version
This command configures the version of IGMP for an interface or range of interfaces. The value for version is either 1, 2, or 3.

Default: 3
Format: ip igmp version version
Modes: Interface Config

8.4.3.1 no ip igmp version
This command resets the version of IGMP to the default value.

Format: no ip igmp version
Modes: Interface Config

8.4.4 ip igmp last-member-query-count
This command sets the number of Group-Specific Queries sent by the interface or range of interfaces before the router assumes that there are no local members on the interface. The range for count is 1 to 20.

Format: ip igmp last-member-query-count count
Modes: Interface Config
8.4.4.1 no ip igmp last-member-query-count
This command resets the number of Group-Specific Queries to the default value.

Format    no ip igmp last-member-query-count
Modes     Interface Config

8.4.5 ip igmp last-member-query-interval
This command configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages. The range for seconds is 0 to 255 tenths of a second. This value can be configured on one interface or a range of interfaces.

Default   10 tenths of a second (1 second)
Format    ip igmp last-member-query-interval seconds
Modes     Interface Config

8.4.5.1 no ip igmp last-member-query-interval
This command resets the Maximum Response Time to the default value.

Format    no ip igmp last-member-query-interval
Modes     Interface Config

8.4.6 ip igmp query-interval
This command configures the query interval for the specified interface or range of interfaces. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for query-interval is 1 to 3600 seconds.

Default   125 seconds
Format    ip igmp query-interval seconds
Modes     Interface Config

8.4.6.1 no ip igmp query-interval
This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format    no ip igmp query-interval
Modes     Interface Config
8.4.7  ip igmp query-max-response-time
This command configures the maximum response time interval for the specified interface or range of interfaces, which is
the maximum query response time advertised in IGMPv2 queries on this interface. The time interval is specified in tenths
of a second. The range for \texttt{gmp query-max-response-time} is 0 to 255 tenths of a second.

Default  100
Format \texttt{ip igmp query-max-response-time 0-255}
Mode  Interface Config

8.4.7.1  no ip igmp query-max-response-time
This command resets the maximum response time interval for the specified interface, which is the maximum query
response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval
is reset to the default time.

Format \texttt{no ip igmp query-max-response-time}
Mode  Interface Config

8.4.8  ip igmp robustness
This command configures the robustness that allows tuning of the interface or range of interfaces. The robustness is the
tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may
be increased for the interface. The range for \texttt{robustness} is 1 to 255.

Default  2
Format \texttt{ip igmp robustness 1-255}
Mode  Interface Config

8.4.8.1  no ip igmp robustness
This command sets the robustness value to default.

Format \texttt{no ip igmp robustness}
Mode  Interface Config

8.4.9  ip igmp startup-query-count
This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface
or range of interfaces. The range for \texttt{count} is 1 to 20.

Default  2
Format \texttt{ip igmp startup-query-count 1-20}
Mode  Interface Config
8.4.9.1  no ip igmp startup-query-count
This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format  no ip igmp startup-query-count
Mode    Interface Config

8.4.10  ip igmp startup-query-interval
This command sets the interval between General Queries sent on startup on the interface or range of interfaces. The time interval value is in seconds. The range for interval is 1 to 300 seconds.

Default  31
Format    ip igmp startup-query-interval 1-300
Mode      Interface Config

8.4.10.1  no ip igmp startup-query-interval
This command resets the interval between General Queries sent on startup on the interface to the default value.

Format    no ip igmp startup-query-interval
Mode      Interface Config

8.4.11  show ip igmp
This command displays the system-wide IGMP information.

Format    show ip igmp
Modes     • Privileged EXEC
          • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Admin Mode</td>
<td>The administrative status of IGMP. This is a configured value.</td>
</tr>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>Indicates whether IGMP is enabled or disabled on the interface. This is a configured value.</td>
</tr>
<tr>
<td>Protocol State</td>
<td>The current state of IGMP on this interface. Possible values are Operational or Non-Operational.</td>
</tr>
</tbody>
</table>

8.4.12  show ip igmp groups
This command displays the registered multicast groups on the interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format. If [detail] is specified this command displays the registered multicast groups on the interface in detail.

Format    show ip igmp groups {slot/port|vlan 1-4093 [detail]}
Mode      Privileged EXEC
If you do not use the `detail` keyword, the following fields appear:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the interface participating in the multicast group.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask of the interface participating in the multicast group.</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>This displays whether IGMP is enabled or disabled on this interface.</td>
</tr>
</tbody>
</table>

The following fields are not displayed if the interface is not enabled:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querier Status</td>
<td>This displays whether the interface has IGMP in Querier mode or Non-Querier mode.</td>
</tr>
<tr>
<td>Groups</td>
<td>The list of multicast groups that are registered on this interface.</td>
</tr>
</tbody>
</table>

If you use the `detail` keyword, the following fields appear:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast IP Address</td>
<td>The IP address of the registered multicast group on this interface.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>The IP address of the source of the last membership report received for the specified multicast group address on this interface.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time elapsed since the entry was created for the specified multicast group address on this interface.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The amount of time remaining to remove this entry before it is aged out.</td>
</tr>
<tr>
<td>Version1 Host Timer</td>
<td>The time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or &quot;-----&quot; if there is no Version 1 host present.</td>
</tr>
<tr>
<td>Version2 Host Timer</td>
<td>The time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or &quot;-----&quot; if there is no Version 2 host present.</td>
</tr>
<tr>
<td>Group Compatibility Mode</td>
<td>The group compatibility mode (v1, v2 or v3) for this group on the specified interface.</td>
</tr>
</tbody>
</table>

### 8.4.13 show ip igmp interface

This command displays the IGMP information for the interface. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of in a `slot/port` format.

**Format**

`show ip igmp interface {slot/port|vlan 1-4093}`

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td><code>slot/port</code></td>
</tr>
<tr>
<td>IGMP Admin Mode</td>
<td>The administrative status of IGMP.</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>Indicates whether IGMP is enabled or disabled on the interface.</td>
</tr>
<tr>
<td>IGMP Version</td>
<td>The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>The frequency at which IGMP Host-Query packets are transmitted on this interface.</td>
</tr>
<tr>
<td>Query Max Response Time</td>
<td>The maximum query response time advertised in IGMPv2 queries on this interface.</td>
</tr>
</tbody>
</table>
8.4.14  show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

**Format**  
```
show ip igmp interface membership multipaddr [detail]
```

**Mode**  
Privileged EXEC

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid unit, slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Interface IP</td>
<td>The IP address of the interface participating in the multicast group.</td>
</tr>
<tr>
<td>State</td>
<td>The interface that has IGMP in Querier mode or Non-Querier mode.</td>
</tr>
<tr>
<td>Group Compatibility Mode</td>
<td>The group compatibility mode (v1, v2 or v3) for the specified group on this interface.</td>
</tr>
<tr>
<td>Source Filter Mode</td>
<td>The source filter mode (Include/Exclude) for the specified group on this interface. This is &quot;---&quot; for IGMPv1 and IGMPv2 Membership Reports.</td>
</tr>
</tbody>
</table>

If you use the **detail** keyword, the following fields appear:

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid unit, slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Group Compatibility Mode</td>
<td>The group compatibility mode (v1, v2 or v3) for the specified group on this interface.</td>
</tr>
<tr>
<td>Source Filter Mode</td>
<td>The source filter mode (Include/Exclude) for the specified group on this interface. This is &quot;---&quot; for IGMPv1 and IGMPv2 Membership Reports.</td>
</tr>
<tr>
<td>Source Hosts</td>
<td>The list of unicast source IP addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP address. This is &quot;-----&quot; for IGMPv1 and IGMPv2 Membership Reports.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The amount of time remaining to remove this entry before it is aged out. This is &quot;-----&quot; for IGMPv1 and IGMPv2 Membership Reports.</td>
</tr>
</tbody>
</table>

8.4.15  show ip igmp interface stats

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

**Format**  
```
show ip igmp interface stats [slot/port|vlan 1-4093]
```

**Modes**  
- Privileged EXEC
- User EXEC
The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

### 8.5.1  ip igmp-proxy
This command enables the IGMP Proxy on the an interface or range of interfaces. To enable the IGMP Proxy on an interface, you must enable multicast forwarding. Also, make sure that there are no multicast routing protocols enabled on the router.

**Format**
```
ip igmp-proxy
```

**Mode**
```
Interface Config
```

### 8.5.1.1  no ip igmp-proxy
This command disables the IGMP Proxy on the router.

**Format**
```
no ip igmp-proxy
```

**Mode**
```
Interface Config
```

### 8.5.2  ip igmp-proxy unsolicit-rprt-interval
This command sets the unsolicited report interval for the IGMP Proxy interface or range of interfaces. This command is valid only when you enable IGMP Proxy on the interface or range of interfaces. The value of `interval` can be 1-260 seconds.

**Default**
```
1
```

**Format**
```
ip igmp-proxy unsolicit-rprt-interval 1-260
```

**Mode**
```
Interface Config
```
8.5.2.1 no ip igmp-proxy unsolicit-rprt-interval
This command resets the unsolicited report interval of the IGMP Proxy router to the default value.

Format: no ip igmp-proxy unsolicit-rprt-interval
Mode: Interface Config

8.5.3 ip igmp-proxy reset-status
This command resets the host interface status parameters of the IGMP Proxy interface (or range of interfaces). This command is valid only when you enable IGMP Proxy on the interface.

Format: ip igmp-proxy reset-status
Mode: Interface Config

8.5.4 show ip igmp-proxy
This command displays a summary of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format: show ip igmp-proxy
Modes: Privileged EXEC, User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface index</td>
<td>The interface number of the IGMP Proxy.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>States whether the IGMP Proxy is enabled or not. This is a configured value.</td>
</tr>
<tr>
<td>Operational Mode</td>
<td>States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.</td>
</tr>
<tr>
<td>Version</td>
<td>The present IGMP host version that is operational on the proxy interface.</td>
</tr>
<tr>
<td>Number of Multicast Groups</td>
<td>The number of multicast groups that are associated with the IGMP Proxy interface.</td>
</tr>
<tr>
<td>Unsolicited Report Interval</td>
<td>The time interval at which the IGMP Proxy interface sends unsolicited group membership report.</td>
</tr>
<tr>
<td>Querier IP Address on Proxy Interface</td>
<td>The IP address of the Querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).</td>
</tr>
<tr>
<td>Older Version 1 Querier Timeout</td>
<td>The interval used to timeout the older version 1 queriers.</td>
</tr>
<tr>
<td>Older Version 2 Querier Timeout</td>
<td>The interval used to timeout the older version 2 queriers.</td>
</tr>
<tr>
<td>Proxy Start Frequency</td>
<td>The number of times the IGMP Proxy has been stopped and started.</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the command.
(FASTPATH Routing) #show ip igmp-proxy
Interface Index................................. 0/1
Admin Mode......................................... Enable
Operational Mode.................................. Enable
Version............................................. 3
Num of Multicast Groups......................... 0
Unsolicited Report Interval.................... 1
Querier IP Address on Proxy Interface........ 5.5.5.50
Older Version 1 Querier Timeout............... 0
Older Version 2 Querier Timeout............... 00:00:00
Proxy Start Frequency......................... 1
8.5.5  show ip igmp-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format    show ip igmp-proxy interface
Modes     • Privileged EXEC
          • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Index</td>
<td>The slot/port of the IGMP proxy.</td>
</tr>
</tbody>
</table>

The column headings of the table associated with the interface are as follows:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ver</td>
<td>The IGMP version.</td>
</tr>
<tr>
<td>Query Rcvd</td>
<td>Number of IGMP queries received.</td>
</tr>
<tr>
<td>Report Rcvd</td>
<td>Number of IGMP reports received.</td>
</tr>
<tr>
<td>Report Sent</td>
<td>Number of IGMP reports sent.</td>
</tr>
<tr>
<td>Leaves Rcvd</td>
<td>Number of IGMP leaves received. Valid for version 2 only.</td>
</tr>
<tr>
<td>Leaves Sent</td>
<td>Number of IGMP leaves sent on the Proxy interface. Valid for version 2 only.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show ip igmp-proxy interface

```
Interface Index................................. 0/1

Ver Query Rcvd Report Rcvd Report Sent Leave Rcvd Leave Sent
1   0    0    0    0           -----     -----     
2   0    0    0    0    0        0          0      
3   0    0    0           -----     -----     
```

8.5.6  show ip igmp-proxy groups

This command displays information about the subscribed multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format    show ip igmp-proxy groups
Modes     • Privileged EXEC
          • User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface number of the IGMP Proxy.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The IP address of the multicast group.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>The IP address of host that last sent a membership report for the current group on the network attached to the IGMP Proxy interface (upstream interface).</td>
</tr>
<tr>
<td>Up Time (in secs)</td>
<td>The time elapsed since last created.</td>
</tr>
<tr>
<td>Member State</td>
<td>The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER.</td>
</tr>
<tr>
<td></td>
<td>• IDLE_MEMBER - interface has responded to the latest group membership query for this group.</td>
</tr>
<tr>
<td></td>
<td>• DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.</td>
</tr>
<tr>
<td>Filter Mode</td>
<td>Possible values are Include or Exclude.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

```
(FASTPATH Routing) #show ip igmp-proxy groups
```

### Interface Index

<table>
<thead>
<tr>
<th>Interface</th>
<th>0/1</th>
</tr>
</thead>
</table>

### Group Address | Last Reporter | Up Time | Member State | Filter Mode | Sources |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>225.4.4.4</td>
<td>5.5.5.48</td>
<td>00:02:21</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>3</td>
</tr>
<tr>
<td>226.4.4.4</td>
<td>5.5.5.48</td>
<td>00:02:21</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>3</td>
</tr>
<tr>
<td>227.4.4.4</td>
<td>5.5.5.48</td>
<td>00:02:21</td>
<td>DELAY_MEMBER</td>
<td>Exclude</td>
<td>0</td>
</tr>
<tr>
<td>228.4.4.4</td>
<td>5.5.5.48</td>
<td>00:02:21</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>3</td>
</tr>
</tbody>
</table>

### 8.5.7 show ip igmp-proxy groups detail

This command displays complete information about multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

#### Format

```
show ip igmp-proxy groups detail
```

#### Modes

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface number of the IGMP Proxy.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The IP address of the multicast group.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>The IP address of host that last sent a membership report for the current group, on the network attached to the IGMP-Proxy interface (upstream interface).</td>
</tr>
<tr>
<td>Up Time (in secs)</td>
<td>The time elapsed since last created.</td>
</tr>
<tr>
<td>Member State</td>
<td>The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER.</td>
</tr>
<tr>
<td>Filter Mode</td>
<td>Possible values are Include or Exclude.</td>
</tr>
<tr>
<td>Sources</td>
<td>The number of sources attached to the multicast group.</td>
</tr>
<tr>
<td>Group Source List</td>
<td>The list of IP addresses of the sources attached to the multicast group.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Time left before a source is deleted.</td>
</tr>
</tbody>
</table>

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

```
(FASTPATH Routing) #show ip igmp-proxy groups
```

### Interface Index

<table>
<thead>
<tr>
<th>Interface</th>
<th>0/1</th>
</tr>
</thead>
</table>

### Group Address | Last Reporter | Up Time | Member State | Filter Mode | Sources |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>225.4.4.4</td>
<td>5.5.5.48</td>
<td>00:02:21</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>3</td>
</tr>
</tbody>
</table>

### Group Source List | Expiry Time
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.2.3</td>
<td>00:02:21</td>
</tr>
</tbody>
</table>
DELAY_MEMBER

<table>
<thead>
<tr>
<th>Group Source List</th>
<th>Expiry Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.2.3</td>
<td>00:02:21</td>
</tr>
<tr>
<td>6.1.2.3</td>
<td>00:01:44</td>
</tr>
<tr>
<td>8.1.2.3</td>
<td>00:01:44</td>
</tr>
<tr>
<td>227.4.4.4</td>
<td>00:02:21</td>
</tr>
<tr>
<td>228.4.4.4</td>
<td>00:03:21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Source List</th>
<th>Expiry Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1.2.3</td>
<td>00:03:21</td>
</tr>
<tr>
<td>6.1.2.3</td>
<td>00:03:21</td>
</tr>
<tr>
<td>7.1.2.3</td>
<td>00:03:21</td>
</tr>
</tbody>
</table>
9/ IPv6 Multicast Commands

This chapter describes the IPv6 Multicast commands available in the FASTPATH CLI.

There is no specific IP multicast enable for IPv6. Enabling of multicast at global config is common for both IPv4 and IPv6.

This chapter contains the following sections:
- "IPv6 Multicast Forwarder" on page 842
- "IPv6 PIM Commands" on page 845
- "IPv6 MLD Commands" on page 857
- "IPv6 MLD-Proxy Commands" on page 862

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.

9.1 IPv6 Multicast Forwarder

9.1.1 ipv6 mroute

This command configures an IPv6 Multicast Static Route for a source.

Default  No MRoute is configured on the system.

Format  ipv6 mroute src-ip-addr src-mask rpf-addr [interface] preference

Parameter Description
-----------------------------------
src-ip-addr  The IP address of the multicast source network.
src-mask  The IP mask of the multicast data source.
rpf-ip-addr  The IP address of the RPF next-hop router toward the source.
interface  Specify the interface if the RPF Address is a link-local address.
preference  The administrative distance for this Static MRoute, that is, the preference value. The range is 1 to 255.
### 9.1.1.1 no ipv6 mroute

This command removes the configured IPv6 Multicast Static Route.

**Format**

`no ip mroute src-ip-addr`

**Mode**

Global Config

### 9.1.2 show ipv6 mroute

Use this command to show the mroute entries specific for IPv6. (This command is the IPv6 equivalent of the IPv4 `show ip mroute` command.)

**Format**

`show ipv6 mroute [detail] [summary] [group {group-address} [detail | summary]] [source {source-address} [grpaddr | summary ]]`

**Modes**

- Privileged EXEC
- User EXEC

If you use the `detail` parameter, the command displays the following Multicast Route Table fields:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The time of expiry of this entry in seconds.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time elapsed since the entry was created in seconds.</td>
</tr>
<tr>
<td>RPF Neighbor</td>
<td>The IP address of the RPF neighbor.</td>
</tr>
<tr>
<td>Flags</td>
<td>The flags associated with this entry.</td>
</tr>
</tbody>
</table>

If you use the `summary` parameter, the command displays the following fields:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The multicast routing protocol by which the entry was created.</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>The interface on which the packet for the source/group arrives.</td>
</tr>
<tr>
<td>Outgoing Interface List</td>
<td>The list of outgoing interfaces on which the packet is forwarded.</td>
</tr>
</tbody>
</table>

### 9.1.3 show ipv6 mroute group

This command displays the multicast configuration settings specific to IPv6 such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given group IPv6 address `group-address`.

**Format**

`show ipv6 mroute group group-address {detail | summary}`

**Modes**

- Privileged EXEC
- User EXEC
9.1.4 show ipv6 mroute source

This command displays the multicast configuration settings specific to IPv6 such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given source IP address or source IP address and group IP address pair.

**Format**

```
show ipv6 mroute source source-address {grpaddr | summary}
```

**Modes**

- Privileged EXEC
- User EXEC

If you use the `groupipaddr` parameter, the command displays the following column headings in the output table:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The time of expiry of this entry in seconds.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time elapsed since the entry was created in seconds.</td>
</tr>
<tr>
<td>RPF Neighbor</td>
<td>The IP address of the RPF neighbor.</td>
</tr>
<tr>
<td>Flags</td>
<td>The flags associated with this entry.</td>
</tr>
</tbody>
</table>

If you use the `summary` parameter, the command displays the following column headings in the output table:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Addr</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP Addr</td>
<td>The IP address of the destination of the multicast packet.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The multicast routing protocol by which this entry was created.</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>The interface on which the packet for this group arrives.</td>
</tr>
<tr>
<td>Outgoing Interface List</td>
<td>The list of outgoing interfaces on which this packet is forwarded.</td>
</tr>
</tbody>
</table>

9.1.5 show ipv6 mroute static

Use the `show ipv6 mroute static` command in Privileged EXEC or User EXEC mode to display all the configured IPv6 multicast static routes.

**Format**

```
show ipv6 mroute static [source-address]
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>IP address of the multicast source network.</td>
</tr>
<tr>
<td>Source Mask</td>
<td>The subnetwork mask pertaining to the sourceIP.</td>
</tr>
</tbody>
</table>
9.1.6 clear ipv6 mroute

This command deletes all or the specified IPv6 multicast route entries.

This command only clears dynamic mroute entries. It does not clear static mroutes.

**Format**
clear ipv6 mroute {*|group-address[ source-address]}

**Modes**
Privileged EXEC

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Deletes all IPv6 entries from the IPv6 multicast routing table.</td>
</tr>
<tr>
<td>group-address</td>
<td>IPv6 address of the multicast group.</td>
</tr>
<tr>
<td>source-address</td>
<td>The IPv6 address of a multicast source that is sending multicast traffic to the group.</td>
</tr>
</tbody>
</table>

**Example:** The following deletes all entries from the IPv6 multicast routing table:
(Broadcom FASTPATH Routing) # clear ipv6 mroute *

**Example:** The following deletes all entries from the IPv6 multicast routing table that match the given multicast group address (FF4E::1), irrespective of which source is sending for this group:
(Broadcom FASTPATH Routing) # clear ipv6 mroute FF4E::1

**Example:** The following deletes all entries from the IPv6 multicast routing table that match the given multicast group address (FF4E::1) and the multicast source address (2001::2):
(Broadcom FASTPATH Routing) # clear ip mroute FF4E::1 2001::2

9.2 IPv6 PIM Commands

This section describes the commands you use to configure Protocol Independent Multicast - Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM) for IPv6 multicast routing. PIM-DM and PIM-SM are multicast routing protocols that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. Only one PIM mode can be operational at a time.

9.2.1 ipv6 pim dense

This command enables the administrative mode of PIM-DM in the router.
**Example:** The following shows an example of the command.

(FASTPATH) (Config) #ipv6 pim dense

9.2.1.1 no ipv6 pim dense
This command disables the administrative mode of PIM-DM in the router.

**Default** disabled
**Format** ipv6 pim dense
**Mode** Global Config

9.2.2 ipv6 pim sparse
This command enables the administrative mode of PIM-SM in the router.

**Default** disabled
**Format** ipv6 pim sparse
**Mode** Global Config

**Example:** The following shows an example of the command.

(FASTPATH) (Config) #ipv6 pim sparse

9.2.2.1 no ipv6 pim sparse
This command disables the administrative mode of PIM-SM in the router.

**Default** disabled
**Format** no ipv6 pim sparse
**Mode** Global Config

9.2.3 ipv6 pim
This command administratively enables PIM on an interface or range of interfaces.

**Default** disabled
**Format** ipv6 pim
**Mode** Interface Config

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

(FASTPATH) (Interface 0/1) #ipv6 pim
9.2.3.1  **no ipv6 pim**

This command sets the administrative mode of PIM on an interface to disabled.

**Format**  
no ipv6 pim

**Mode**  
Interface Config

## 9.2.4  **ipv6 pim hello-interval**

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces. The hello-interval is specified in seconds and is in the range 0–18000.

**Default**  
30

**Format**  
ipv6 pim hello-interval 0–18000

**Mode**  
Interface Config

**Example:** The following shows an example of the command.

(FASTPATH) (Interface 0/1) #ipv6 pim hello-interval 50

### 9.2.4.1  **no ipv6 pim hello-interval**

Use this command to set the PIM hello interval to the default value.

**Format**  
no ipv6 pim hello-interval

**Mode**  
Interface Config

## 9.2.5  **ipv6 pim bsr-border**

Use this command to prevent bootstrap router (BSR) messages from being sent or received on the specified interface.

This command takes effect only when PIM-SM is enabled in the Global mode.

**Default**  
disabled

**Format**  
ipv6 pim bsr-border

**Mode**  
Interface Config

**Example:** The following shows an example of the command.

(FASTPATH) (Interface 0/1) #ipv6 pim bsr-border
9.2.5.1 no ipv6 pim bsr-border

Use this command to disable the setting of BSR border on the specified interface.

**Format**

no ipv6 pim bsr-border

**Mode**

Interface Config

9.2.6 ipv6 pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR). The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

---

**NOTICE**

This command takes effect only when PIM-SM is configured as the PIM mode.

---

**Default**

Disabled

**Format**

ipv6 pim bsr-candidate interface {slot/port|vlan 1-4093} hash-mask-length [bsr-priority] [interval interval]

**Mode**

Global Config

---

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Interface number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with PIM.</td>
</tr>
<tr>
<td>hash-mask-length</td>
<td>Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.</td>
</tr>
<tr>
<td>bsr-priority</td>
<td>Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR. The default value is 0.</td>
</tr>
<tr>
<td>interval</td>
<td>[Optional] Indicates the BSR candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.</td>
</tr>
</tbody>
</table>

**Example:** The following shows examples of the command.

(FASTPATH) (Config) #ip pim bsr-candidate interface 0/1 32 5

(FASTPATH) (Config) #ip pim bsr-candidate interface 0/1 32 5 interval 100
9.2.6.1 **no ipv6 pim bsr-candidate**  
This command is used to remove the configured PIM Candidate BSR router.

**Format**  
no ipv6 pim bsr-candidate interface {slot/port|vlan 1-4093} hash-mask-length [priority]

**Mode**  
Global Config

9.2.7 **ipv6 pim dr-priority**  
Use this command to set the priority value for which a router is elected as the designated router (DR).

---

**NOTICE**  
This command takes effect only when PIM-SM is enabled in the Global mode.

**Default**  
1

**Format**  
ipv6 pim dr-priority 0-2147483647

**Mode**  
Interface Config

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

(FASTPATH) (Interface 0/1) #ipv6 pim dr-priority 10

9.2.7.1 **no ipv6 pim dr-priority**  
Use this command to return the DR Priority on the specified interface to its default value.

**Format**  
no ipv6 pim dr-priority

**Mode**  
Interface Config

9.2.8 **ipv6 pim join-prune-interval**  
This command is used to configure the join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

---

**NOTICE**  
This command takes effect only when PIM-SM is enabled in the Global mode.

**Default**  
60

**Format**  
ipv6 pim join-prune-interval 0-18000

**Mode**  
Interface Config

**Example:** The following shows examples of the command.

(FASTPATH) (Interface 0/1) #ipv6 pim join-prune-interval 90
9.2.8.1 no ipv6 pim join-prune-interval

Use this command to set the join/prune interval on the specified interface to the default value.

**Format**

```
no ipv6 pim join-prune-interval
```

**Mode**

Interface Config

9.2.9 ipv6 pim rp-address

This command defines the address of a PIM Rendezvous point (RP) for a specific multicast group range.

---

**NOTICE**
This command takes effect only when PIM-SM is configured as the PIM mode.

**Default**

0

**Format**

```
ipv6 pim rp-address rp-address group-address/prefix-length [override]
```

**Mode**

Global Config

**Parameter** | **Description**
--- | ---
rp-address | The IPv6 address of the RP.
group-address | The group address supported by the RP.
group-mask | The group mask for the group address.
override | [Optional] Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

**Example:** The following shows an example of the command.

```
(FASTPATH) (Config) #ip pim rp-address 192.168.10.1 224.1.2.0 255.255.255.0
```

9.2.9.1 no ipv6 pim rp-address

This command is used to remove the address of the configured PIM Rendezvous point (RP) for the specified multicast group range.

**Format**

```
no ipv6 pim rp-address rp-address group-address group-mask [override]
```

**Mode**

Global Config

9.2.10 ipv6 pim rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR) for a specific multicast group range. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

---

**NOTICE**
This command takes effect only when PIM-SM is configured as the PIM mode.

**Default**

Disabled

**Format**

```
ipv6 pim rp-candidate interface {slot/port|vlan 1-4093} group-address group-mask [interval interval]
```

**Mode**

Global Config
Example: The following shows examples of the command.

(FASTPATH) (Config) #ipv6 pim rp-candidate interface 0/1 224.1.2.0 255.255.255.0
(FASTPATH) (Config) #ipv6 pim rp-candidate interface 0/1 224.1.2.0 255.255.255.0 interval 200

9.2.10.1 no ipv6 pim rp-candidate
This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format
no ipv6 pim rp-candidate interface {slot/port|vlan 1-4093} group-address group-mask

Mode
Global Config

9.2.11 ipv6 pim ssm
Use this command to define the Source Specific Multicast (SSM) range of IPv6 multicast addresses on the router.

Example: The following shows an example of the command.

(Fastpath) (Config) #ipv6 pim ssm default
(Fastpath) (Config) #ipv6 pim ssm 232.1.2.0 255.255.255.0

Parameter | Description
--- | ---
slot/port | The IP address associated with this interface type and number is advertised as a candidate RP address. This interface must be enabled with PIM.
group-address | The multicast group address that is advertised in association with the RP address.
group-mask | The multicast group prefix that is advertised in association with the RP address.
interval | [Optional] Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

default-range | Defines the SSM range access list FF3x::/32.
9.2.11.1  no ipv6 pim ssm
Use this command to remove the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

**Format**

no ipv6 pim ssm {default | group-address group-mask}

**Mode**

Global Config

9.2.12  show ipv6 pim
This command displays the system-wide information for PIM-DM or PIM-SM.

**Format**

show ipv6 pim

**Modes**

- Privileged EXEC
- User EXEC

---

**NOTICE**

If the PIM mode is PIM-DM (dense), some of the fields in the following table do not display in the command output because they are applicable only to PIM-SM.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM Mode</td>
<td>Indicates whether the PIM mode is dense (PIM-DM) or sparse (PIM-SM)</td>
</tr>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>Indicates whether PIM is enabled or disabled on this interface.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The current state of PIM on this interface: Operational or Non-Operational.</td>
</tr>
</tbody>
</table>

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

Example #1: PIM Mode - Dense
(FASTPATH) #show ip pim

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface-Mode</th>
<th>Operational-Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Enabled</td>
<td>Operational</td>
</tr>
<tr>
<td>0/3</td>
<td>Disabled</td>
<td>Non-Operational</td>
</tr>
</tbody>
</table>

Example #2: PIM Mode - Sparse
(FASTPATH) #show ip pim

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface-Mode</th>
<th>Operational-Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Enabled</td>
<td>Operational</td>
</tr>
<tr>
<td>0/3</td>
<td>Disabled</td>
<td>Non-Operational</td>
</tr>
</tbody>
</table>

Example #3: PIM Mode - None
(FASTPATH) #show ip pim

PIM Mode None

None of the routing interfaces are enabled for PIM.
9.2.13  show ipv6 pim ssm  
This command displays the configured source specific IPv6 multicast addresses. If no SSM Group range is configured, this command output is No SSM address range is configured.

Format  
show ipv6 pim ssm  

Modes  
- Privileged EXEC  
- User EXEC  

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The IPv6 multicast address of the SSM group.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>The network prefix length.</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the command.  
(FASTPATH) #show ip pim ssm  

Group Address/Prefix Length  
-----------------------------  
232.0.0.0/8  

If no SSM Group range is configured, this command displays the following message:  
No SSM address range is configured.  

9.2.14  show ipv6 pim interface  
This command displays the interface information for PIM on the specified interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Format  
show ipv6 pim interface [{slot/port|vlan 1-4093}]  

Modes  
- Privileged EXEC  
- User EXEC  

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Mode</td>
<td>Indicates whether the PIM mode enabled on the interface is dense or sparse.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.</td>
</tr>
<tr>
<td>Join Prune Interval</td>
<td>The join/prune interval for the PIM router. The interval is in seconds.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense</td>
</tr>
<tr>
<td>BSR Border</td>
<td>Identifies whether this interface is configured as a bootstrap router border interface.</td>
</tr>
<tr>
<td>Neighbor Count</td>
<td>The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(FASTPATH) #show ipv6 pim interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Hello Interval (secs)</th>
<th>Join Prune Interval (secs)</th>
<th>DR Priority</th>
<th>BSR Border</th>
<th>Neighbor Count</th>
<th>Designated Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>Sparse</td>
<td>30</td>
<td>60</td>
<td>1</td>
<td>Disabled</td>
<td>1</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>0/2</td>
<td>Sparse</td>
<td>30</td>
<td>60</td>
<td>1</td>
<td>Disabled</td>
<td>1</td>
<td>192.168.10.1</td>
</tr>
</tbody>
</table>

If none of the interfaces are enabled for PIM, the following message is displayed:

None of the routing interfaces are enabled for PIM.

9.2.15 show ipv6 pim neighbor

This command displays PIM neighbors discovered by PIMv2 Hello messages. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format. If the interface number is not specified, this command displays the neighbors discovered on all the PIM-enabled interfaces.

Format: show ipv6 pim neighbor [{slot/port|vlan 1-4093}]

Modes:
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Address</td>
<td>The IPv6 address of the PIM neighbor on an interface.</td>
</tr>
<tr>
<td>Interface</td>
<td>slot/port</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time since this neighbor has become active on this interface.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Time remaining for the neighbor to expire.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>The DR Priority configured on this interface (PIM-SM only).</td>
</tr>
</tbody>
</table>

Note: DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

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

(FASTPATH) #show ipv6 pim neighbor

<table>
<thead>
<tr>
<th>Neighbor Addr</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expiry Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8:39::/32</td>
<td>0/1</td>
<td>00:02:55</td>
<td>00:01:15</td>
</tr>
<tr>
<td>2001:DB8:A3::/32</td>
<td>0/2</td>
<td>00:03:50</td>
<td>00:02:10</td>
</tr>
</tbody>
</table>

If no neighbors have been learned on any of the interfaces, the following message is displayed:

No neighbors are learnt on any interface.
9.2.16 show ipv6 pim bsr-router

This command displays the bootstrap router (BSR) information.

**Format**  
show ipv6 pim bsr-router {candidate | elected}

**Mode**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSR Address</td>
<td>IPv6 address of the BSR.</td>
</tr>
<tr>
<td>BSR Priority</td>
<td>Priority as configured in the ipv6 pim bsr-candidate command.</td>
</tr>
<tr>
<td>BSR Hash Mask Length</td>
<td>Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the ipv6 pim bsr-candidate command.</td>
</tr>
<tr>
<td>C-BSR Advertisement Interval</td>
<td>Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.</td>
</tr>
<tr>
<td>Next Bootstrap Message</td>
<td>Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.</td>
</tr>
</tbody>
</table>

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

(FASTPATH) #show ipv6 pim bsr-router candidate

Example #1:

(FASTPATH) #show ip pim bsr-router elected

BSR Address ........................................... 192.168.10.1  
BSR Priority ....................................... 0  
BSR Hash Mask Length ............................... 30  
Next Bootstrap message (hh:mm:ss) ........... 00:00:24

Example #2:

(FASTPATH) #show ip pim bsr-router candidate

BSR Address ........................................... 192.168.10.1  
BSR Priority ....................................... 0  
BSR Hash Mask Length ............................... 30  
C-BSR Advertisement Interval (secs) ....... 60  
Next Bootstrap message (hh:mm:ss) ......... NA

If no configured or elected BSRs exist on the router, the following message is displayed:

No BSR's exist/learned on this router.

9.2.17 show ipv6 pim rp-hash

This command displays which rendezvous point (RP) is being used for a specified group.

**Format**  
show ipv6 pim rp-hash group-address

**Modes**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>The IPv6 address of the RP for the group specified.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the mechanism (BSR or static) by which the RP was selected.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(FASTPATH) #show ip pim rp-hash 224.1.2.0

RP Address 192.168.10.1
Type Static

If no RP Group mapping exist on the router, the following message is displayed:
No RP-Group mappings exist/learned on this router.

9.2.18 show ipv6 pim rp mapping

Use this command to display the mapping for the PIM group to the active Rendezvous points (RP) of which the router is aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address or to view group-to-candidate RP or group to Static RP mapping information.

Example: The following show examples of CLI display output for the command.

Example #1:

(FASTPATH) #show ipv6 pim rp mapping 192.168.10.1

RP Address 192.168.10.1
Group Address 224.1.2.1
Group Mask 255.255.255.0
Origin Static

Example #2:

(FASTPATH) #show ipv6 pim rp mapping candidate

RP Address 192.168.20.1
Group Address 229.2.0.0
Group Mask 255.255.0.0
Origin Static

Example #3:

(FASTPATH) # show ipv6 pim rp mapping candidate

C-RP Advertisement Interval (secs)........ 60
Next Candidate RP Advertisement (hh:mm:ss). 00:00:15

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>The IPv6 address of the RP for the group specified.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The IPv6 address and prefix length of the multicast group.</td>
</tr>
<tr>
<td>Origin</td>
<td>Indicates the mechanism (BSR or static) by which the RP was selected.</td>
</tr>
</tbody>
</table>
| C-RP Advertisement    | Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.
| Interval              | C-RP Advertisement Interval (secs)........ 60
| Next Candidate RP     | Next Candidate RP Advertisement (hh:mm:ss). 00:00:15

Term | Definition
---|---------------------------------------------------------------
RP Address | The IPv6 address of the RP for the group specified.
Group Address | The IPv6 address and prefix length of the multicast group.
Origin | Indicates the mechanism (BSR or static) by which the RP was selected.
C-RP Advertisement Interval | Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.
If no RP Group mapping exist on the router, the following message is displayed:

No RP-Group mappings exist on this router.

9.3 IPv6 MLD Commands

IGMP/MLD Snooping is Layer 2 functionality but IGMP/MLD are Layer 3 multicast protocols. It requires that in a network setup there should be a multicast router (which can act as a querier) to be present to solicit the multicast group registrations. However some network setup does not need a multicast router as multicast traffic is destined to hosts within the same network. In this situation, FASTPATH has an IGMP/MLD Snooping Querier running on one of the switches and Snooping enabled on all the switches. For more information, see "IGMP Snooping Configuration Commands" on page 449 and "MLD Snooping Commands" on page 460.

9.3.1 ipv6 mld router

Use this command, in the administrative mode of the router, to enable MLD in the router.

**Default** Disabled

**Format** `ipv6 mld router`

**Mode** Global Config

9.3.1.1 no ipv6 mld router

Use this command, in the administrative mode of the router, to disable MLD in the router.

**Default** Disabled

**Format** `no ipv6 mld router`

**Mode** Global Config

9.3.2 ipv6 mld query-interval

Use this command to set the MLD router’s query interval for the interface or range of interfaces. The query-interval is the amount of time between the general queries sent when the router is the querier on that interface. The range for `query-interval` is 1 to 3600 seconds.

**Default** 125

**Format** `ipv6 mld query-interval query-interval`

**Mode** Interface Config
9.3.2.1  no ipv6 mld query-interval
Use this command to reset the MLD query interval to the default value for that interface.

Format  no ipv6 mld query-interval
Mode    Interface Config

9.3.3   ipv6 mld query-max-response-time
Use this command to set the MLD querier’s maximum response time for the interface or range of interfaces and this
value is used in assigning the maximum response time in the query messages that are sent on that interface. The range
for query-max-response-time is 0 to 65535 milliseconds.

Default  10000 milliseconds
Format    ipv6 mld query-max-response-time query-max-response-time
Mode      Interface Config

9.3.3.1  no ipv6 mld query-max-response-time
This command resets the MLD query max response time for the interface to the default value.

Format  no ipv6 mld query-max-response-time
Mode    Interface Config

9.3.4   ipv6 mld last-member-query-interval
Use this command to set the last member query interval for an MLD interface or range of interfaces, which is the value of
the maximum response time parameter in the group specific queries sent out of this interface. The range for last-
member-query-interval is 0 to 65535 milliseconds.

Default  1000 milliseconds
Format    ipv6 mld last-member-query-interval last-member-query-interval
Mode      Interface Config
9.3.4.1  no ipv6 mld last-member-query-interval
Use this command to reset the \textit{last-member-query-interval} parameter of the interface to the default value.

Format  no ipv6 mld last-member-query-interval
Mode    Interface Config

9.3.5  ipv6 mld last-member-query-count
Use this command to set the number of listener-specific queries sent before the router assumes that there are no local members on an interface or range of interfaces. The range for \textit{last-member-query-count} is 1 to 20.

Default  2
Format    ipv6 mld last-member-query-count \textit{last-member-query-count}
Mode      Interface Config

9.3.5.1  no ipv6 mld last-member-query-count
Use this command to reset the \textit{last-member-query-count} parameter of the interface to the default value.

Format    no ipv6 mld last-member-query-count
Mode      Interface Config

9.3.6  ipv6 mld version
Use this command to configure the MLD version that the interface uses.

Default  2
Format    ipv6 mld version \{ 1 \ | \ 2 \}
Mode      Interface Config

9.3.6.1  no ipv6 mld version
This command resets the MLD version used by the interface to the default value.

Format    no ipv6 mld
Mode      Interface Config

9.3.7  show ipv6 mld groups
Use this command to display information about multicast groups that MLD reported. The information is displayed only when MLD is enabled on at least one interface. If MLD was not enabled on even one interface, there is no group information to be displayed. The argument \textit{slot/port} corresponds to a physical routing interface or VLAN routing interface. The keyword \textit{vlan} is used to specify the VLAN ID of the routing VLAN directly instead of in a \textit{slot/port} format.

Format    show ipv6 mld groups \{slot/port|vlan 1-4093\|\textit{group-address}\}
Mode      • Privileged EXEC
          • User EXEC
The following fields are displayed as a table when slot/port is specified.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The address of the multicast group.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the multicast group is reachable.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Time elapsed in hours, minutes, and seconds since the multicast group has been known.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Time left in hours, minutes, and seconds before the entry is removed from the MLD membership table.</td>
</tr>
</tbody>
</table>

When group-address is specified, the following fields are displayed for each multicast group and each interface.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface through which the multicast group is reachable.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The address of the multicast group.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>The IP Address of the source of the last membership report received for this multicast group address on that interface.</td>
</tr>
<tr>
<td>Filter Mode</td>
<td>The filter mode of the multicast group on this interface. The values it can take are include and exclude.</td>
</tr>
<tr>
<td>Version 1 Host</td>
<td>The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.</td>
</tr>
<tr>
<td>Group Compat Mode</td>
<td>The compatibility mode of the multicast group on this interface. The values it can take are MLDv1 and MLDv2.</td>
</tr>
</tbody>
</table>

The following table is displayed to indicate all the sources associated with this group.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>The IP address of the source.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time elapsed in hours, minutes, and seconds since the source has been known.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Time left in hours, minutes, and seconds before the entry is removed.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show ipv6 mld groups ?

```
group-address Enter Group Address Info.
<slot/port> Enter interface in slot/port format.
```

(FASTPATH Routing) #show ipv6 mld groups 0/1

```
Group Address................................. FF43::3
Interface........................................ 0/1
Up Time (hh:mm:ss).............................. 00:03:04
Expiry Time (hh:mm:ss)........................... ------
```

(FASTPATH Routing) #show ipv6 mld groups ff43::3

```
Interface........................................ 0/1
Group Address.................................... FF43::3
Last Reporter.................................... FE80::200:FF:FE00:3
Up Time (hh:mm:ss).............................. 00:02:53
Expiry Time (hh:mm:ss)........................... ------
Filter Mode....................................... Include
Version1 Host Timer............................... ------
Group compat mode............................... v2
Source Address Expirey Time
```

www.kontron.com
9.3.8 show ipv6 mld interface

Use this command to display MLD-related information for the interface. The argument slot/port corresponds to a physical routing interface or VLAN routing interface. The keyword vlan is used to specify the VLAN ID of the routing VLAN directly instead of in a slot/port format.

**Format**

```
show ipv6 mld interface {slot/port|vlan 1-4093}
```

**Mode**

- Privileged EXEC
- User EXEC

The following information is displayed for each of the interfaces or for only the specified interface.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface number in slot/port format.</td>
</tr>
<tr>
<td>MLD Mode</td>
<td>Displays the configured administrative status of MLD.</td>
</tr>
<tr>
<td>Operational Mode</td>
<td>The operational status of MLD on the interface.</td>
</tr>
<tr>
<td>MLD Version</td>
<td>Indicates the version of MLD configured on the interface.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>Indicates the configured query interval for the interface.</td>
</tr>
<tr>
<td>Robustness</td>
<td>Displays the configured value for the tuning for the expected packet loss on a subnet attached to the interface.</td>
</tr>
<tr>
<td>Startup Query Interval</td>
<td>This value indicates the configured interval between General Queries sent by a Querier on startup.</td>
</tr>
<tr>
<td>Startup Query Count</td>
<td>This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.</td>
</tr>
<tr>
<td>Last Member Query Interval</td>
<td>This value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.</td>
</tr>
<tr>
<td>Last Member Query Count</td>
<td>This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.</td>
</tr>
</tbody>
</table>

The following information is displayed if the operational mode of the MLD interface is enabled.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querier Status</td>
<td>This value indicates whether the interface is an MLD querier or non-querier on the subnet it is associated with.</td>
</tr>
<tr>
<td>Querier Address</td>
<td>The IP address of the MLD querier on the subnet the interface is associated with.</td>
</tr>
<tr>
<td>Querier Up Time</td>
<td>Time elapsed in seconds since the querier state has been updated.</td>
</tr>
<tr>
<td>Querier Expiry Time</td>
<td>Time left in seconds before the Querier loses its title as querier.</td>
</tr>
<tr>
<td>Wrong Version Queries</td>
<td>Indicates the number of queries received whose MLD version does not match the MLD version of the interface.</td>
</tr>
<tr>
<td>Number of Joins</td>
<td>The number of times a group membership has been added on this interface.</td>
</tr>
<tr>
<td>Number of Leaves</td>
<td>The number of times a group membership has been removed on this interface.</td>
</tr>
<tr>
<td>Number of Groups</td>
<td>The current number of membership entries for this interface.</td>
</tr>
</tbody>
</table>
9.3.9 show ipv6 mld traffic
Use this command to display MLD statistical information for the router.

Format: show ipv6 mld traffic
Mode: Privileged EXEC, User EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid MLD Packets Received</td>
<td>The number of valid MLD packets received by the router.</td>
</tr>
<tr>
<td>Valid MLD Packets Sent</td>
<td>The number of valid MLD packets sent by the router.</td>
</tr>
<tr>
<td>Queries Received</td>
<td>The number of valid MLD queries received by the router.</td>
</tr>
<tr>
<td>Queries Sent</td>
<td>The number of valid MLD queries sent by the router.</td>
</tr>
<tr>
<td>Reports Received</td>
<td>The number of valid MLD reports received by the router.</td>
</tr>
<tr>
<td>Reports Sent</td>
<td>The number of valid MLD reports sent by the router.</td>
</tr>
<tr>
<td>Leaves Received</td>
<td>The number of valid MLD leaves received by the router.</td>
</tr>
<tr>
<td>Leaves Sent</td>
<td>The number of valid MLD leaves sent by the router.</td>
</tr>
<tr>
<td>Bad Checksum MLD Packets</td>
<td>The number of bad checksum MLD packets received by the router.</td>
</tr>
<tr>
<td>Malformed MLD Packets</td>
<td>The number of malformed MLD packets received by the router.</td>
</tr>
</tbody>
</table>

9.3.10 clear ipv6 mld counters
Use this command to reset the MLD counters to zero on the specified interface.

Format: clear ipv6 mld slot/port
Mode: Privileged EXEC

9.3.11 clear ipv6 mld traffic
Use this command to clear all entries in the MLD traffic database.

Format: clear ipv6 mld slot/port
Mode: Privileged EXEC

9.4 IPv6 MLD-Proxy Commands
MLD-Proxy is the IPv6 equivalent of IGMP-Proxy. MLD-Proxy commands allow you to configure the network device as well as to view device settings and statistics using either serial interface or telnet session. The operation of MLD-Proxy commands is the same as for IGMP-Proxy: MLD is for IPv6 and IGMP is for IPv4. MGMD is a term used to refer to both IGMP and MLD.

9.4.1 ipv6 mld-proxy
Use this command to enable MLD-Proxy on the interface or range of interfaces. To enable MLD-Proxy on the interface, you must enable multicast forwarding. Also, make sure that there are no other multicast routing protocols enabled on the router.

Format: ipv6 mld-proxy
Mode: Interface Config
9.4.1  no ipv6 mld-proxy
Use this command to disable MLD-Proxy on the router.

Format          no ipv6 mld-proxy
Mode            Interface Config

9.4.2  ipv6 mld-proxy unsolicit-rprt-interval
Use this command to set the unsolicited report interval for the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface. The value of interval is 1-260 seconds.

Default         1
Format          ipv6 mld-proxy unsolicit-rprt-interval interval
Mode            Interface Config

9.4.2.1  no ipv6 mld-proxy unsolicited-report-interval
Use this command to reset the MLD-Proxy router’s unsolicited report interval to the default value.

Format          no ipv6 mld-proxy unsolicit-rprt-interval
Mode            Interface Config

9.4.3  ipv6 mld-proxy reset-status
Use this command to reset the host interface status parameters of the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface.

Format          ipv6 mld-proxy reset-status
Mode            Interface Config

9.4.4  show ipv6 mld-proxy
Use this command to display a summary of the host interface status parameters.

Format          show ipv6 mld-proxy
Mode            • Privileged EXEC
                • User EXEC

The command displays the following parameters only when you enable MLD-Proxy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Index</td>
<td>The interface number of the MLD-Proxy.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>Indicates whether MLD-Proxy is enabled or disabled. This is a configured value.</td>
</tr>
<tr>
<td>Operational Mode</td>
<td>Indicates whether MLD-Proxy is operationally enabled or disabled. This is a status parameter.</td>
</tr>
<tr>
<td>Version</td>
<td>The present MLD host version that is operational on the proxy interface.</td>
</tr>
<tr>
<td>Number of Multicast Groups</td>
<td>The number of multicast groups that are associated with the MLD-Proxy interface.</td>
</tr>
<tr>
<td>Unsolicited Report Interval</td>
<td>The time interval at which the MLD-Proxy interface sends unsolicited group membership report.</td>
</tr>
<tr>
<td>Querier IP Address on Proxy Interface</td>
<td>The IP address of the Querier, if any, in the network attached to the upstream interface (MLD-Proxy interface).</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(FASTPATH Routing) #show ipv6 mld-proxy

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Index</td>
<td>The slot/port of the MLD-proxy.</td>
</tr>
</tbody>
</table>

The column headings of the table associated with the interface are as follows:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ver</td>
<td>The MLD version.</td>
</tr>
<tr>
<td>Query Rcvd</td>
<td>Number of MLD queries received.</td>
</tr>
<tr>
<td>Report Rcvd</td>
<td>Number of MLD reports received.</td>
</tr>
<tr>
<td>Report Sent</td>
<td>Number of MLD reports sent.</td>
</tr>
<tr>
<td>Leaves Rcvd</td>
<td>Number of MLD leaves received. Valid for version 2 only.</td>
</tr>
<tr>
<td>Leaves Sent</td>
<td>Number of MLD leaves sent on the Proxy interface. Valid for version 2 only.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show ipv6 mld-proxy interface

<table>
<thead>
<tr>
<th>Interface Index</th>
<th>0/1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ver</td>
<td></td>
</tr>
<tr>
<td>Query Rcvd</td>
<td>1</td>
</tr>
<tr>
<td>Report Rcvd</td>
<td>2</td>
</tr>
<tr>
<td>Report Sent</td>
<td>3</td>
</tr>
<tr>
<td>Leaves Rcvd</td>
<td>0</td>
</tr>
<tr>
<td>Leaves Sent</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable MLD-Proxy.

**Format**

- show ipv6 mld-proxy interface

**Modes**

- Privileged EXEC
- User EXEC
9.4.6  show ipv6 mld-proxy groups

Use this command to display information about multicast groups that the MLD-Proxy reported.

**Format**  
show ipv6 mld-proxy groups

**Mode**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface number of the MLD-Proxy.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The IP address of the multicast group.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).</td>
</tr>
<tr>
<td>Up Time (in secs)</td>
<td>The time elapsed in seconds since last created.</td>
</tr>
<tr>
<td>Member State</td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Idle_Member. The interface has responded to the latest group membership query for this group.</td>
</tr>
<tr>
<td></td>
<td>• Delay_Member. The interface is going to send a group membership report to respond to a group membership query for this group.</td>
</tr>
<tr>
<td>Filter Mode</td>
<td>Possible values are Include or Exclude.</td>
</tr>
<tr>
<td>Sources</td>
<td>The number of sources attached to the multicast group.</td>
</tr>
</tbody>
</table>

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

(FASTPATH Routing) #show ipv6 mld-proxy groups

Interface Index................. 0/3

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Last Reporter</th>
<th>Up Time</th>
<th>Member State</th>
<th>Filter Mode</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF1E::1</td>
<td>FE80::100:2.3</td>
<td>00:01:40</td>
<td>DELAY_MEMBER</td>
<td>Exclude</td>
<td>2</td>
</tr>
<tr>
<td>FF1E::2</td>
<td>FE80::100:2.3</td>
<td>00:02:40</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>1</td>
</tr>
<tr>
<td>FF1E::3</td>
<td>FE80::100:2.3</td>
<td>00:01:40</td>
<td>DELAY_MEMBER</td>
<td>Exclude</td>
<td>0</td>
</tr>
<tr>
<td>FF1E::4</td>
<td>FE80::100:2.3</td>
<td>00:02:44</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>4</td>
</tr>
</tbody>
</table>

9.4.7  show ipv6 mld-proxy groups detail

Use this command to display information about multicast groups that MLD-Proxy reported.

**Format**  
show ipv6 mld-proxy groups detail

**Mode**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface number of the MLD-Proxy.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The IP address of the multicast group.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).</td>
</tr>
<tr>
<td>Up Time (in secs)</td>
<td>The time elapsed in seconds since last created.</td>
</tr>
</tbody>
</table>
**Example:** The following shows example CLI display output for the command.

(FASTPATH Routing) #show ipv6 igmp-proxy groups

<table>
<thead>
<tr>
<th>Interface Index</th>
<th>0/3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Address</strong></td>
<td><strong>Last Reporter</strong></td>
</tr>
<tr>
<td>FF1E::1</td>
<td>FE80::100:2:3</td>
</tr>
<tr>
<td><strong>Group Source List</strong></td>
<td><strong>Expiry Time</strong></td>
</tr>
<tr>
<td>2001::1</td>
<td></td>
</tr>
<tr>
<td>2001::2</td>
<td></td>
</tr>
<tr>
<td>FF1E::2</td>
<td>FE80::100:2:3</td>
</tr>
<tr>
<td><strong>Group Source List</strong></td>
<td><strong>Expiry Time</strong></td>
</tr>
<tr>
<td>3001::1</td>
<td></td>
</tr>
<tr>
<td>3002::2</td>
<td></td>
</tr>
<tr>
<td>FF1E::3</td>
<td>FE80::100:2:3</td>
</tr>
<tr>
<td>FF1E::4</td>
<td>FE80::100:2:3</td>
</tr>
<tr>
<td><strong>Group Source List</strong></td>
<td><strong>Expiry Time</strong></td>
</tr>
<tr>
<td>4001::1</td>
<td></td>
</tr>
<tr>
<td>5002::2</td>
<td></td>
</tr>
</tbody>
</table>

**Field**

<table>
<thead>
<tr>
<th><strong>Member State</strong></th>
<th>Possible values are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle_Member</td>
<td>The interface has responded to the latest group membership query for this group.</td>
</tr>
<tr>
<td>Delay_Member</td>
<td>The interface is going to send a group membership report to respond to a group membership query for this group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Filter Mode</strong></th>
<th>Possible values are Include or Exclude.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources</td>
<td>The number of sources attached to the multicast group.</td>
</tr>
<tr>
<td>Group Source List</td>
<td>The list of IP addresses of the sources attached to the multicast group.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The time left for a source to get deleted.</td>
</tr>
</tbody>
</table>
10/ 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. The most recent log messages are displayed first.

**NOTICE**

This chapter is not a complete list of all syslog messages.

The Log Messages chapter includes the following sections:

- “Core” on page 867
- “Utilities” on page 869
- “Management” on page 872
- “Switching” on page 876
- “QoS” on page 883
- “Routing/IPv6 Routing” on page 884
- “Multicast” on page 887
- “Technologies” on page 892
- “O/S Support” on page 894

10.1 Core

Table 15: BSP Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSP</td>
<td>Event(0xaaaaaaaa)</td>
<td>Switch has restarted.</td>
</tr>
<tr>
<td>BSP</td>
<td>Starting code...</td>
<td>BSP initialization complete, starting FAST-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PATH application.</td>
</tr>
</tbody>
</table>

Table 16: NIM Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIM</td>
<td>NIM: L7_ATTACH out of order for interface unit x slot x port x</td>
<td>Interface creation out of order.</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: L7_DETACH out of order for interface unit x slot x port x</td>
<td>Interface creation out of order.</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: L7_DELETE out of order for interface unit x slot x port x</td>
<td>Interface creation out of order.</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: event(x),intf(x),component(x), in wrong phase</td>
<td>An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: Failed to notify users of interface change</td>
<td>Event was not propagated to the system.</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: failed to send message to NIM message Queue.</td>
<td>NIM message queue full or non-existent.</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: Failed to notify the components of L7_CREATE event</td>
<td>Interface not created.</td>
</tr>
</tbody>
</table>
Table 16: NIM Log Messages (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIM</td>
<td>NIM: Attempted event (x), on USP x.x.x before phase 3</td>
<td>A component issued an interface event during the wrong initialization phase.</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: incorrect phase for operation</td>
<td>An API call was made during the wrong initialization phase.</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: Component(x) failed on event(x) for interface</td>
<td>A component responded with a fail indication for an interface event.</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: Timeout event(x), interface remaining-Mask = xxxx</td>
<td>A component did not respond before the NIM timeout occurred.</td>
</tr>
</tbody>
</table>

Table 17: SIM Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIM</td>
<td>IP address conflict on service port/network port for IP address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx</td>
<td>This message appears when an address conflict is detected in the LAN for the service port/network port IP.</td>
</tr>
</tbody>
</table>

Table 18: System Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>Configuration file fastpath.cfg size is 0 (zero) bytes</td>
<td>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.</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>could not separate SYSAPI_CONFIG_FILE-NAMENAME</td>
<td>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.</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>Building defaults for file file name version version num</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 10.2 Utilities

#### Table 19: Trap Mgr Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Mgr</td>
<td>Link Up/Down: slot/port</td>
<td>An interface changed link state.</td>
</tr>
</tbody>
</table>

#### Table 20: DHCP Filtering Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Filtering</td>
<td>Unable to create r/w lock for DHCP Filtering</td>
<td>Unable to create semaphore used for dhcp filtering configuration structure.</td>
</tr>
<tr>
<td>DHCP Filtering</td>
<td>Failed to register with nv Store.</td>
<td>Unable to register save and restore functions for configuration save.</td>
</tr>
<tr>
<td>DHCP Filtering</td>
<td>Failed to register with NIM</td>
<td>Unable to register with NIM for interface callback functions.</td>
</tr>
<tr>
<td>DHCP Filtering</td>
<td>Error on call to sysapiCfgFileWrite file</td>
<td>Error on trying to save configuration.</td>
</tr>
</tbody>
</table>
### Table 21: NVStore Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVStore</td>
<td>Building defaults for file XXX</td>
<td>A component’s configuration file does not exist or the file’s checksum is incorrect so the component’s default configuration file is built.</td>
</tr>
<tr>
<td>NVStore</td>
<td>Error on call to osapiFsWrite routine on file XXX</td>
<td>Either the file cannot be opened or the OS’s file I/O returned an error trying to write to the file.</td>
</tr>
<tr>
<td>NVStore</td>
<td>File XXX corrupted from file system. Checksum mismatch.</td>
<td>The calculated checksum of a component’s configuration file in the file system did not match the checksum of the file in memory.</td>
</tr>
<tr>
<td>NVStore</td>
<td>Migrating config file XXX from version Y to Z</td>
<td>A configuration file version mismatch was detected so a configuration file migration has started.</td>
</tr>
</tbody>
</table>

### Table 22: RADIUS Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>RADIUS: Invalid data length - xxx</td>
<td>The RADIUS Client received an invalid message from the server.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Failed to send the request</td>
<td>A problem communicating with the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Failed to send all of the request</td>
<td>A problem communicating with the RADIUS server during transmit.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Could not get the Task Sync semaphore!</td>
<td>Resource issue with RADIUS Client service.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Buffer is too small for response processing</td>
<td>RADIUS Client attempted to build a response larger than resources allow.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Could not allocate accounting requestInfo</td>
<td>Resource issue with RADIUS Client service.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Could not allocate requestInfo</td>
<td>Resource issue with RADIUS Client service.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: osapiSocketRecvFrom returned error</td>
<td>Error while attempting to read data from the RADIUS server.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Accounting-Response failed to validate, id = xxx</td>
<td>The RADIUS Client received an invalid message from the server.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: User (xxx) needs to respond for challenge</td>
<td>An unexpected challenge was received for a configured user.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Could not allocate a buffer for the packet</td>
<td>Resource issue with RADIUS Client service.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Access-Challenge failed to validate, id = xxx</td>
<td>The RADIUS Client received an invalid message from the server.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Failed to validate Message-Authenticator, id = xxx</td>
<td>The RADIUS Client received an invalid message from the server.</td>
</tr>
</tbody>
</table>
### Table 22: RADIUS Log Messages (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>RADIUS: Access-Accept failed to validate, id = xxx</td>
<td>The RADIUS Client received an invalid message from the server.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Invalid packet length – xxx</td>
<td>The RADIUS Client received an invalid message from the server.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Response is missing Message-Authenticator, id = xxx</td>
<td>The RADIUS Client received an invalid message from the server.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS: Server address doesn't match configured server</td>
<td>RADIUS Client received a server response from an unconfigured server.</td>
</tr>
</tbody>
</table>

### Table 23: TACACS+ Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+</td>
<td>TACACS+: authentication error, no server to contact</td>
<td>TACACS+ request needed, but no servers are configured.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>TACACS+: connection failed to server x.x.x.x</td>
<td>TACACS+ request sent to server x.x.x.x but no response was received.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>TACACS+: no key configured to encrypt packet for server x.x.x.x</td>
<td>No key configured for the specified server.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>TACACS+: received invalid packet type from server.</td>
<td>Received packet type that is not supported.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>TACACS+: invalid major version in received packet.</td>
<td>Major version mismatch.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>TACACS+: invalid minor version in received packet.</td>
<td>Minor version mismatch.</td>
</tr>
</tbody>
</table>

### Table 24: LLDP Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP</td>
<td>lldpTask(): invalid message type:xx. xxxxxxx:xx</td>
<td>Unsupported LLDP packet received.</td>
</tr>
</tbody>
</table>

### Table 25: SNTP Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNTP</td>
<td>SNTP: system clock synchronized on %s UTC</td>
<td>Indicates that SNTP has successfully synchronized the time of the box with the server.</td>
</tr>
</tbody>
</table>
Table 26: DHCPv6 Client Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP6 Client</td>
<td>ip6Map dhcp add failed.</td>
<td>This message appears when the update of a DHCP leased IP address to IP6Map fails.</td>
</tr>
<tr>
<td>DHCP6 Client</td>
<td>osapiNetAddrV6Add failed on interface xxx.</td>
<td>This message appears when the update of a DHCP leased IP address to the kernel IP Stack fails.</td>
</tr>
<tr>
<td>DHCP6 Client</td>
<td>Failed to add DNS Server xxx to DNS Client.</td>
<td>This message appears when the update of a DNS6 Server address given by the DHCPv6 Server to the DNS6 Client fails.</td>
</tr>
<tr>
<td>DHCP6 Client</td>
<td>Failed to add Domain name xxx to DNS Client.</td>
<td>This message appears when the update of a DNS6 Domain name info given by the DHCPv6 Server to the DNS6 Client fails.</td>
</tr>
</tbody>
</table>

Table 27: DHCPv4 Client Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP4 Client</td>
<td>Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt</td>
<td>This message appears when a message is received from the DHCP Server that contains an un-supported Vendor Option.</td>
</tr>
<tr>
<td>DHCP4 Client</td>
<td>Failed to acquire an IP address on xxx; DHCP Server did not respond.</td>
<td>This message appears when the DHCP Client fails to lease an IP address from the DHCP Server.</td>
</tr>
<tr>
<td>DHCP4 Client</td>
<td>DNS name server entry add failed.</td>
<td>This message appears when the update of a DNS Domain name server info given by the DHCP Server to the DNS Client fails.</td>
</tr>
<tr>
<td>DHCP4 Client</td>
<td>DNS domain name list entry addition failed.</td>
<td>This message appears when the update of a DNS Domain name list info given by the DHCP Server to the DNS Client fails.</td>
</tr>
<tr>
<td>DHCP4 Client</td>
<td>Interface xxx Link State is Down. Connect the port and try again.</td>
<td>This message appears when the Network protocol is configured with DHCP without any active links in the Management VLAN.</td>
</tr>
</tbody>
</table>

10.3 Management

Table 28: SNMP Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>EDB Callback: Unit Join: x.</td>
<td>A new unit has joined the stack.</td>
</tr>
</tbody>
</table>
### Table 29: EmWeb Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmWeb</td>
<td>EMWEB (Telnet): Max number of Telnet login sessions exceeded</td>
<td>A user attempted to connect via telnet when the maximum number of telnet sessions were already active.</td>
</tr>
<tr>
<td>EmWeb</td>
<td>EMWEB (SSH): Max number of SSH login sessions exceeded</td>
<td>A user attempted to connect via SSH when the maximum number of SSH sessions were already active.</td>
</tr>
<tr>
<td>EmWeb</td>
<td>Handle table overflow</td>
<td>All the available EmWeb connection handles are being used and the connection could not be made.</td>
</tr>
<tr>
<td>EmWeb</td>
<td>ConnectionType EmWeb socket accept() failed: errno</td>
<td>Socket accept failure for the specified connection type.</td>
</tr>
<tr>
<td>EmWeb</td>
<td>EmWeb: connection allocation failed</td>
<td>Memory allocation failure for the new connection.</td>
</tr>
<tr>
<td>EmWeb</td>
<td>EMWEB TransmitPending: EWOULDBLOCK error sending data</td>
<td>Socket error on send.</td>
</tr>
<tr>
<td>EmWeb</td>
<td>ewsNetHTTPEnd: internal error - handle not in Handle table</td>
<td>EmWeb handle index not valid.</td>
</tr>
<tr>
<td>EmWeb</td>
<td>ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!</td>
<td>The receive buffer limit has been reached. Bad request or DoS attack.</td>
</tr>
<tr>
<td>EmWeb</td>
<td>EmWeb accept: XXXX</td>
<td>Accept function for new SSH connection failed. XXXX indicates the error info.</td>
</tr>
</tbody>
</table>

### Table 30: CLI_UTIL Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI_UTIL</td>
<td>Telnet Send Failed errno = 0x%lx</td>
<td>Failed to send text string to the telnet client.</td>
</tr>
<tr>
<td>CLI_UTIL</td>
<td>osapiFsDir failed</td>
<td>Failed to obtain the directory information from a volume's directory.</td>
</tr>
</tbody>
</table>
Table 31: WEB Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEB</td>
<td>Max clients exceeded</td>
<td>This message is shown when the maximum allowed java client connections to the switch is exceeded.</td>
</tr>
<tr>
<td>WEB</td>
<td>Error on send to sockfd XXXX, closing connection</td>
<td>Failed to send data to the java clients through the socket.</td>
</tr>
<tr>
<td>WEB</td>
<td># (XXXX) Form Submission Failed. No Action Taken.</td>
<td>The form submission failed and no action is taken. XXXX indicates the file under consideration.</td>
</tr>
<tr>
<td>WEB</td>
<td>ewaFormServe_file_download() - WEB Unknown return code from tftp download result</td>
<td>Unknown error returned while downloading file using TFTP from web interface.</td>
</tr>
<tr>
<td>WEB</td>
<td>ewaFormServe_file_upload() - Unknown return code from tftp upload result</td>
<td>Unknown error returned while uploading file using TFTP from web interface.</td>
</tr>
<tr>
<td>WEB</td>
<td>Web UI Screen with unspecified access attempted to be brought up</td>
<td>Failed to get application-specific authorization handle provided to EmWeb/Server by the application in ewsAuthRegister(). The specified web page will be served in read-only mode.</td>
</tr>
</tbody>
</table>

Table 32: CLI_WEB_MGR Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI_WEB_MGR</td>
<td>File size is greater than 2K</td>
<td>The banner file size is greater than 2K bytes.</td>
</tr>
<tr>
<td>CLI_WEB_MGR</td>
<td>No. of rows greater than allowed maximum of XXXX</td>
<td>When the number of rows exceeds the maximum allowed rows.</td>
</tr>
</tbody>
</table>

Table 33: SSHD Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSHD</td>
<td>SSHD: Unable to create the global (data) semaphore</td>
<td>Failed to create semaphore for global data protection.</td>
</tr>
<tr>
<td>SSHD</td>
<td>SSHD: Msg Queue is full, event = XXXX</td>
<td>Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent.</td>
</tr>
<tr>
<td>SSHD</td>
<td>SSHD: Unknown UI event in message, event = XXXX</td>
<td>Failed to dispatch the UI event to the appropriate SSHD function as it’s an invalid event. XXXX indicates the event to be dispatched.</td>
</tr>
<tr>
<td>SSHD</td>
<td>sshdApiCnfgrCommand: Failed calling sshdIssueCmd.</td>
<td>Failed to send the message to the SSHD message queue.</td>
</tr>
</tbody>
</table>
### Table 34: SSLT Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLT</td>
<td>SSLT: Exceeded maximum, ssltConnection-Task</td>
<td>Exceeded maximum allowed SSLT connections.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Error creating Secure server socket6</td>
<td>Failed to create secure server socket for IPV6.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Can’t connect to unsecure server at XXXX, result = YYY, errno = ZZZZ</td>
<td>Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYY is the result returned from connect function and ZZZZ is the error code.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Msg Queue is full, event = XXXX</td>
<td>Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Unknown UI event in message, event = XXXX</td>
<td>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.</td>
</tr>
<tr>
<td>SSLT</td>
<td>ssltApiCnfgrCommand: Failed calling ssltIssueCmd.</td>
<td>Failed to send the message to the SSLT message queue.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Error loading certificate from file XXXX</td>
<td>Failed while loading the SSL certificate from specified file. XXXX indicates the file from where the certificate is being read.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Error loading private key from file</td>
<td>Failed while setting private key for SSL connection.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Error setting cipher list (no valid ciphers)</td>
<td>Failed to delete SSL semaphores during cleanup of all resources associated with the OpenSSL Locking semaphores.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Could not delete the SSL semaphores</td>
<td>Failed to delete SSL semaphores during cleanup of all resources associated with the OpenSSL Locking semaphores.</td>
</tr>
</tbody>
</table>

### Table 35: User_Manager Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>User_Manager</td>
<td>User Login Failed for XXXX</td>
<td>Failed to authenticate user login. XXXX indicates the username to be authenticated.</td>
</tr>
<tr>
<td>User_Manager</td>
<td>Access level for user XXXX could not be determined. Setting to Level 1.</td>
<td>Invalid access level specified for the user. The access level is set to Level 1. XXXX indicates the username.</td>
</tr>
<tr>
<td>User_Manager</td>
<td>Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.</td>
<td>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.</td>
</tr>
</tbody>
</table>
## 10.4 Switching

### Table 36: Protected Ports Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected Ports</td>
<td>Protected Port: failed to save configuration</td>
<td>This appears when the protected port configuration cannot be saved.</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port</td>
<td>This appears when protectedPortCfgRW-Lock Fails.</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback</td>
<td>This appears when nimRegisterIntfChange with VLAN fails.</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>Cannot add interface xxx to group yyy</td>
<td>This appears when an interface could not be added to a particular group.</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>unable to set protected port group</td>
<td>This appears when a dtl call fails to add interface mask at the driver level.</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>Cannot delete interface xxx from group yyy</td>
<td>This appears when a dtl call to delete an interface from a group fails.</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>Cannot update group YYY after deleting interface XXX</td>
<td>This message appears when an update group for an interface deletion fails.</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>Received an interface change callback while not ready to receive it</td>
<td>This appears when an interface change call back has come before the protected port component is ready.</td>
</tr>
</tbody>
</table>

### Table 37: IP Subnet VLANS Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP subnet VLANS</td>
<td>ERROR vlanIpSubnetSubnetValid:Invalid subnet</td>
<td>This occurs when an invalid pair of subnet and netmask has come from the CLI.</td>
</tr>
<tr>
<td>IP subnet VLANS</td>
<td>IP Subnet Vlans: failed to save configuration</td>
<td>This message appears when save configuration of subnet vlans failed.</td>
</tr>
<tr>
<td>IP subnet VLANS</td>
<td>vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet</td>
<td>This appears when a read/write lock creations fails.</td>
</tr>
<tr>
<td>IP subnet VLANS</td>
<td>vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback</td>
<td>This appears when this component unable to register for vlan change notifications.</td>
</tr>
<tr>
<td>IP subnet VLANS</td>
<td>vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore</td>
<td>This appears when a semaphore deletion of this component fails.</td>
</tr>
<tr>
<td>IP subnet VLANS</td>
<td>vlanIpSubnetDtlVlanCreate: Failed</td>
<td>This appears when a dtl call fails to add an entry into the table.</td>
</tr>
<tr>
<td>IP subnet VLANS</td>
<td>vlanIpSubnetSubnetDeleteApply: Failed</td>
<td>This appears when a dtl fails to delete an entry from the table.</td>
</tr>
<tr>
<td>IP subnet VLANS</td>
<td>vlanIpSubnetVlanChangeCallback: Failed to add an Entry</td>
<td>This appears when a dtl fails to add an entry for a vlan add notify event.</td>
</tr>
<tr>
<td>IP subnet VLANS</td>
<td>vlanIpSubnetVlanChangeCallback: Failed to delete an Entry</td>
<td>This appears when a dtl fails to delete an entry for an vlan delete notify event.</td>
</tr>
</tbody>
</table>
### Table 38: Mac-based VLANs Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC based VLANs</td>
<td>MAC VLANs: Failed to save configuration</td>
<td>This message appears when save configuration of Mac vlans failed.</td>
</tr>
<tr>
<td>MAC based VLANs</td>
<td>vlanMacCfgInitPhase1Process: Unable to create r/w lock for vlanMac</td>
<td>This appears when a read/write lock creations fails.</td>
</tr>
<tr>
<td>MAC based VLANs</td>
<td>Unable to register for VLAN change callback</td>
<td>This appears when this component unable to register for vlan change notifications.</td>
</tr>
<tr>
<td>MAC based VLANs</td>
<td>vlanMacCfgFiniPhase1Process: could not delete avl semaphore</td>
<td>This appears when a semaphore deletion of this component fails.</td>
</tr>
<tr>
<td>MAC based VLANs</td>
<td>vlanMacAddApply: Failed to add an entry</td>
<td>This appears when a dtl call fails to add an entry into the table.</td>
</tr>
<tr>
<td>MAC based VLANs</td>
<td>vlanMacDeleteApply: Unable to delete an Entry</td>
<td>This appears when a dtl fails to delete an entry from the table.</td>
</tr>
<tr>
<td>MAC based VLANs</td>
<td>vlanMacVlanChangeCallback: Failed to add an entry</td>
<td>This appears when a dtl fails to add an entry for a vlan add notify event.</td>
</tr>
<tr>
<td>MAC based VLANs</td>
<td>vlanMacVlanChangeCallback: Failed to delete an entry</td>
<td>This appears when a dtl fails to delete an entry for an vlan delete notify event.</td>
</tr>
</tbody>
</table>

### Table 39: 802.1X Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>function: Failed calling dot1xIssueCmd</td>
<td>802.1X message queue is full.</td>
</tr>
<tr>
<td>802.1X</td>
<td>function: EAP message not received from server</td>
<td>RADIUS server did not send required EAP message.</td>
</tr>
<tr>
<td>802.1X</td>
<td>function: Out of System buffers</td>
<td>802.1X cannot process/transmit message due to lack of internal buffers.</td>
</tr>
<tr>
<td>802.1X</td>
<td>function: could not set state to authorized/unauthorized, intf xxx</td>
<td>DTL call failed setting authorization state of the port.</td>
</tr>
<tr>
<td>802.1X</td>
<td>dot1xApplyConfigData: Unable to enable/disable dot1x in driver</td>
<td>DTL call failed enabling/disabling 802.1X.</td>
</tr>
<tr>
<td>802.1X</td>
<td>dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed</td>
<td>Failed sending message to RADIUS server.</td>
</tr>
<tr>
<td>802.1X</td>
<td>dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx</td>
<td>Failed sending accounting start to RADIUS server.</td>
</tr>
<tr>
<td>802.1X</td>
<td>function: failed sending terminate cause, intf xxx</td>
<td>Failed sending accounting stop to RADIUS server.</td>
</tr>
</tbody>
</table>
### Table 40: IGMP Snooping Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping</td>
<td>function: osapiMessageSend failed</td>
<td>IGMP Snooping message queue is full.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>Failed to set global igmp snooping mode to xxx</td>
<td>Failed to set global IGMP Snooping mode due to message queue being full.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>Failed to set igmp snooping mode xxx for interface yyy</td>
<td>Failed to set interface IGMP Snooping mode due to message queue being full.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>Failed to set igmp mrouter mode xxx for interface yyy</td>
<td>Failed to set interface multicast router mode due to IGMP Snooping message queue being full.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>Failed to set igmp snooping mode xxx for vlan yyy</td>
<td>Failed to set VLAN IGMP Snooping mode due to message queue being full.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>Failed to set igmp mrouter mode%d for interface xxx on_vlan yyy</td>
<td>Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>snoopCnfgrInitPhase1Process: Error allocating small buffers</td>
<td>Could not allocate buffers for small IGMP packets.</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>snoopCnfgrInitPhase1Process: Error allocating large buffers</td>
<td>Could not allocate buffers for large IGMP packets.</td>
</tr>
</tbody>
</table>

### Table 41: GARP/GVRP/GMRP Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>GARP/GVRP/GMRP</td>
<td>garpSpanState, garpIfStateChange, GarpIsssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:</td>
<td>The garpQueue is full, logs specifics of the message content like internal interface number, type of message, etc.</td>
</tr>
<tr>
<td>GARP/GVRP/GMRP</td>
<td>GarpSendPDU: QUEUE SEND FAILURE</td>
<td>The garpPduQueue is full, logs specific of the GPDU, internal interface number, vlan id, buffer handle, etc.</td>
</tr>
<tr>
<td>GARP/GVRP/GMRP</td>
<td>garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/ GMRP config data for interface %d in garpMapIntfIsConfigurable.</td>
<td>A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.</td>
</tr>
<tr>
<td>GARP/GVRP/GMRP</td>
<td>garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent</td>
<td>Traces the build up of message queue. Helpful in determining the load on GARP.</td>
</tr>
<tr>
<td>GARP/GVRP/GMRP</td>
<td>gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X</td>
<td>Mismatch between the gmd (gmrp database) and MFDB.</td>
</tr>
<tr>
<td>GARP/GVRP/GMRP</td>
<td>gmd_create_entry: GMRP failure adding MFDB entry: vlan %d and address %s</td>
<td>MFDB table is full.</td>
</tr>
</tbody>
</table>
### Table 42: 802.3ad Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.3ad</td>
<td>dot3adReceiveMachine: received default event %x</td>
<td>Received a LAG PDU and the RX state machine is ignoring this LAGPDU.</td>
</tr>
<tr>
<td>802.3ad</td>
<td>dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)</td>
<td>The event sent to NiM was not completed successfully.</td>
</tr>
</tbody>
</table>

### Table 43: FDB Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDB</td>
<td>fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d</td>
<td>Unable to set the age time in the hardware.</td>
</tr>
</tbody>
</table>

### Table 44: Double VLAN Tag Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Double Vlan Tag</td>
<td>dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d</td>
<td>A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.</td>
</tr>
</tbody>
</table>

### Table 45: IPv6 Provisioning Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6 Provisioning</td>
<td>ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d</td>
<td>A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.</td>
</tr>
</tbody>
</table>

### Table 46: MFDB Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFDB</td>
<td>mfdbTreeEntryUpdate: entry does not exist</td>
<td>Trying to update a non existing entry.</td>
</tr>
</tbody>
</table>
### 802.1Q Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q</td>
<td>dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue</td>
<td>dot1qMsgQueue is full.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range.</td>
<td>This accommodates for reserved vlan ids. i.e. 4094 - x.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.</td>
<td>A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dot1qVlanDeleteProcess: Deleting the default VLAN</td>
<td>Typically encountered during clear Vlan and clear config.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dot1qVlanMemberSetModify, dot1qVlan-TaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static</td>
<td>If this vlan is a learnt via GVRP then we cannot modify its member set via management.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dtt failure when adding ports to vlan id %d - portMask = %s</td>
<td>Failed to add the ports to VLAN entry in hardware.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dtt failure when deleting ports from vlan id %d - portMask = %s</td>
<td>Failed to delete the ports for a VLAN entry from the hardware.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dtt failure when adding ports to tagged list for vlan id %d - portMask = %s</td>
<td>Failed to add the port to the tagged list in hardware.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dtt failure when deleting ports from tagged list for vlan id %d - portMask = %s*</td>
<td>Failed to delete the port to the tagged list from the hardware.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x</td>
<td>Failed to receive the dot1q message from dot1q message queue.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!</td>
<td>Failed to create VLAN ID, VLAN Database reached maximum values.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Attempt to create a vlan (%d) that already exists</td>
<td>Creation of the existing Dynamic VLAN ID from the CLI.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>DTL call to create VLAN %d failed with rc %d*</td>
<td>Failed to create VLAN ID in hardware.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Problem unrolling data for VLAN %d</td>
<td>Failed to delete VLAN from the VLAN database after failure of VLAN hardware creation.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Vlan %d does not exist</td>
<td>Failed to delete VLAN entry.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Vlan %d requestor type %d does not exist</td>
<td>Failed to delete dynamic VLAN ID if the given requestor is not valid.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Can not delete the VLAN, Some unknown component has taken the ownership!</td>
<td>Failed to delete, as some unknown component has taken the ownership.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Not valid permission to delete the VLAN %d requestor %d</td>
<td>Failed to delete the VLAN ID as the given requestor and VLAN entry status are not same.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>VLAN Delete Call failed in driver for vlan %d</td>
<td>Failed to delete VLAN ID from the hardware.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Problem deleting data for VLAN %d</td>
<td>Failed to delete VLAN ID from the VLAN database.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Dynamic entry %d can only be modified after it is converted to static</td>
<td>Failed to modify the VLAN group filter.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Cannot find vlan %d to convert it to static</td>
<td>Failed to convert Dynamic VLAN to static VLAN. VLAN ID not exists.</td>
</tr>
<tr>
<td>Component</td>
<td>Message</td>
<td>Cause</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Only Dynamically created VLANs can be converted</td>
<td>Error while trying to convert the static created VLAN ID to static.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Cannot modify tagging of interface %s to non existence vlan %d</td>
<td>Error for a given interface sets the tagging property for all the VLANs in the vlan mask.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Error in updating data for VLAN %d in VLAN database</td>
<td>Failed to add VLAN entry into VLAN database.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>DTL call to create VLAN %d failed with rc %d</td>
<td>Failed to add VLAN entry in hardware.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Not valid permission to delete the VLAN %d</td>
<td>Failed to delete static VLAN ID. Invalid requestor.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Attempt to set access vlan with invalid vlan id %d</td>
<td>Invalid VLAN ID.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Attempt to set access vlan with (%d) that does not exist</td>
<td>VLAN ID not exists.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>VLAN create currently underway for VLAN ID %d</td>
<td>Creating a VLAN which is already under process of creation.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>VLAN ID %d is already exists as static VLAN</td>
<td>Trying to create already existing static VLAN ID.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Cannot put a message on dot1q msg Queue, Returns:%d</td>
<td>Failed to send Dot1q message on Dot1q message Queue.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Invalid dot1q Interface: %s</td>
<td>Failed to add VLAN to a member of port.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Cannot set membership for user interface %s on management vlan %d</td>
<td>Failed to add VLAN to a member of port.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s</td>
<td>Incorrect tagmode for VLAN tagging.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Cannot set tagging for interface %d on non existent VLAN %d</td>
<td>The VLAN ID does not exist.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Cannot set tagging for interface %d which is not a member of VLAN %d</td>
<td>Failure in Setting the tagging configuration for a interface on a range of VLAN.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>VLAN create currently underway for VLAN ID %d</td>
<td>Trying to create the VLAN ID which is already under process of creation.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>VLAN ID %d already exists</td>
<td>Trying to create the VLAN ID which is already exists.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Failed to delete, Default VLAN %d cannot be deleted</td>
<td>Trying to delete Default VLAN ID.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Failed to delete, VLAN ID %d is not a static VLAN</td>
<td>Trying to delete Dynamic VLAN ID from CLI.</td>
</tr>
<tr>
<td>802.1Q</td>
<td>Requestor %d attempted to release internal VLAN %d: owned by %d</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 48: 802.1S Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1S</td>
<td>dot1sIssueCmd: Dot1s Msg Queue is full!!! Event: %u, on interface: %u, for instance: %u</td>
<td>The message Queue is full.</td>
</tr>
<tr>
<td>802.1S</td>
<td>dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded</td>
<td>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.</td>
</tr>
<tr>
<td>802.1S</td>
<td>dot1sBpduTransmit(): could not get a buffer</td>
<td>Out of system buffers.</td>
</tr>
</tbody>
</table>

### Table 49: Port Mac Locking Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Mac Locking</td>
<td>pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.</td>
<td>A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.</td>
</tr>
</tbody>
</table>

### Table 50: Protocol-based VLANs Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Based VLANs</td>
<td>pbVlanCnfgrInitPhase2Process: Unable to register NIM callback</td>
<td>Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.</td>
</tr>
<tr>
<td>Protocol Based VLANs</td>
<td>pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with VLANs</td>
<td>Appears when VLANRegisterForChange fails to register pbVlan for VLAN changes.</td>
</tr>
<tr>
<td>Protocol Based VLANs</td>
<td>pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore</td>
<td>Appears when nvStoreRegister fails to register save and restore functions for configuration save.</td>
</tr>
</tbody>
</table>
## 10.5 QoS

### Table 51: ACL Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Total number of ACL rules (x) exceeds max (y) on intf i.</td>
<td>The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.</td>
</tr>
<tr>
<td>ACL</td>
<td>ACL name, rule x: This rule is not being logged</td>
<td>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.</td>
</tr>
<tr>
<td>ACL</td>
<td>aclLogTask: error logging ACL rule trap for correlator number</td>
<td>The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.</td>
</tr>
<tr>
<td>ACL</td>
<td>IP ACL number: Forced truncation of one or more rules during config migration</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 52: CoS Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS</td>
<td>cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults</td>
<td>The COS component was unable to apply the saved configuration and has initialized to the factory default settings.</td>
</tr>
</tbody>
</table>

### Table 53: DiffServ Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiffServ</td>
<td>diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device</td>
<td>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.</td>
</tr>
<tr>
<td>DiffServ</td>
<td>Policy invalid for service intf: policy name, interface x, direction y</td>
<td>The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.</td>
</tr>
</tbody>
</table>
10.6 Routing/IPv6 Routing

Table S4: DHCP Relay Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP relay</td>
<td>REQUEST hops field more than config value</td>
<td>The DHCP relay agent has processed a DHCP request whose HOPS field is larger than the maximum value allowed. The relay agent will not forward a message with a hop count greater than 4.</td>
</tr>
<tr>
<td>DHCP relay</td>
<td>Request’s seconds field less than the config value</td>
<td>The DHCP relay agent has processed a DHCP request whose SECS field is larger than the configured minimum wait time allowed.</td>
</tr>
</tbody>
</table>
| DHCP relay | processDhcpPacket: invalid DHCP packet type: %u
 | The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent. |

Table S5: OSPFv2 Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv2</td>
<td>Best route client deregistration failed for OSPF Redist</td>
<td>OSPFv2 registers with the IPv4 routing table manager (“RTO”) to be notified of best route changes. There are cases where OSPFv2 deregisters more than once, causing the second deregistration to fail. The failure is harmless.</td>
</tr>
<tr>
<td>OSPFv2</td>
<td>XX_Call() failure in _checkTimers for thread 0x869bcc0</td>
<td>An OSPFv2 timer has fired but the message queue that holds the event has filled up. This is normally a fatal error.</td>
</tr>
<tr>
<td>OSPFv2</td>
<td>Warning: OSPF LSDB is 90% full (22648 LSAs).</td>
<td>OSPFv2 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv2 logs this warning. The warning includes the current size of the database.</td>
</tr>
<tr>
<td>OSPFv2</td>
<td>The number of LSAs, 25165, in the OSPF LSDB has exceeded the LSDB memory allocation.</td>
<td>When the OSPFv2 LSDB becomes full, OSPFv2 logs this message. OSPFv2 reoriginates its router LSAs with the metric of all non-stub links set to the maximum value to encourage other routers to not compute routes through the overloaded router.</td>
</tr>
<tr>
<td>OSPFv2</td>
<td>Dropping the DD packet because of MTU mismatch</td>
<td>OSPFv2 ignored a Database Description packet whose MTU is greater than the IP MTU on the interface where the DD was received.</td>
</tr>
<tr>
<td>OSPFv2</td>
<td>LSA Checksum error in LsUpdate, dropping LSID 1.2.3.4 checksum 0x1234.</td>
<td>OSPFv2 ignored a received link state advertisement (LSA) whose checksum was incorrect.</td>
</tr>
</tbody>
</table>
### Table 56: OSPFv3 Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OSPFv3</strong></td>
<td>Best route client deregistration failed for OSPFv3 Redist</td>
<td>OSPFv3 registers with the IPv6 routing table manager (“RTO6”) to be notified of best route changes. There are cases where OSPFv3 deregisters more than once, causing the second deregistration to fail. The failure is harmless.</td>
</tr>
<tr>
<td><strong>OSPFv3</strong></td>
<td>Warning: OSPF LSDB is 90% full (15292 LSAs).</td>
<td>OSPFv3 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv3 logs this warning. The warning includes the current size of the database.</td>
</tr>
<tr>
<td><strong>OSPFv3</strong></td>
<td>The number of LSAs, 16992, in the OSPF LSDB have exceeded the LSDB memory allocation.</td>
<td>When the OSPFv3 LSDB becomes full, OSPFv3 logs this message. OSPFv3 reoriginates its router LSAs with the R-bit clear indicating that OSPFv3 is overloaded.</td>
</tr>
<tr>
<td><strong>OSPFv3</strong></td>
<td>LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.</td>
<td>OSPFv3 periodically verifies the checksum of each LSA in memory. OSPFv3 logs this.</td>
</tr>
</tbody>
</table>

### Table 57: Routing Table Manager Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RTO</strong></td>
<td>RTO is no longer full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes.</td>
<td>When the number of best routes drops below full capacity, RTO logs this notice. The number of bad adds may give an indication of the number of route adds that failed while RTO was full, but a full routing table is only one reason why this count is incremented.</td>
</tr>
<tr>
<td><strong>RTO</strong></td>
<td>RTO is full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes. The routing table manager stores a limited number of best routes. The count of total routes includes alternate routes, which are not installed in hardware.</td>
<td>The routing table manager, also called “RTO,” stores a limited number of best routes, based on hardware capacity. When the routing table becomes full, RTO logs this alert. The count of total routes includes alternate routes, which are not installed in hardware.</td>
</tr>
</tbody>
</table>
### Table 58: VRRP Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP</td>
<td>VRRP packet of size xxx dropped. Min VRRP packet size is xxx; Max VRRP packet size is xxx.</td>
<td>This message appears when there is flood of VRRP messages in the network.</td>
</tr>
<tr>
<td>VRRP</td>
<td>VR xxx on interface xxx started as xxx.</td>
<td>This message appears when the Virtual router is started in the role of a Master or a Backup.</td>
</tr>
<tr>
<td>VRRP</td>
<td>This router is the IP address owner for virtual router xxx on interface xxx. Setting the virtual router priority to xxx.</td>
<td>This message appears when the address ownership status for a specific VR is updated. If this router is the address owner for the VR, set the VR's priority to MAX priority (as per RFC 3768). If the router is no longer the address owner, revert the priority.</td>
</tr>
</tbody>
</table>

### Table 59: ARP Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>IP address conflict on interface xxx for IP address yyy. Conflicting host MAC address is zzz.</td>
<td>When an address conflict is detected for any IP address on the switch upon reception of ARP packet from another host or router.</td>
</tr>
</tbody>
</table>

### Table 60: RIP Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP</td>
<td>RIP: discard response from xxx via unexpected interface</td>
<td>When RIP response is received with a source address not matching the incoming interface’s subnet.</td>
</tr>
</tbody>
</table>
## 10.7 Multicast

### Table 61: IGMP/MLD Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP/MLD</td>
<td>MGMD Protocol Heap Memory Init Failed; Family – xxx.</td>
<td>MGMD Heap memory initialization Failed for the specified address family. This message appears when trying to enable MGMD Protocol.</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>MGMD Protocol Heap Memory De-Init Failed; Family – xxx.</td>
<td>MGMD Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable MGMD (IGMP/MLD) Protocol. As a result of this, the subsequent attempts to enable/disable MGMD will also fail.</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>MGMD Protocol Initialization Failed; Family – xxx.</td>
<td>MGMD protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable MGMD Protocol.</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>MGMD All Routers Address - xxx Set to the DTL Mcast List Failed; Mode – xxx, intf – xxx.</td>
<td>This message appears when trying to enable/disable MGMD Protocol.</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>MGMD All Routers Address - xxx Add to the DTL Mcast List Failed.</td>
<td>MGMD All Routers Address addition to the local multicast list Failed. As a result of this, MGMD Multicast packets with this address will not be received at the application.</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>MGMD All Routers Address – xxx Delete from the DTL Mcast List Failed.</td>
<td>MGMD All Routers Address deletion from the local multicast list Failed. As a result of this, MGMD Multicast packets are still received at the application though MGMD is disabled.</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>MLDv2 GroupAddr-[FF02::16] Enable with Interpeak Stack Failed; rtrIfNum - xxx, intf – xxx.</td>
<td>Registration of this Group address with the Interpeak stack failed. As a result of this, MLDv2 packets will not be received at the application.</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>MGMD Group Entry Creation Failed; grpAddr - xxx, rtrIfNum – xxx.</td>
<td>The specified Group Address registration on the specified router interface failed.</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>MGMD Socket Creation/Initialization Failed for addrFamily – xxx.</td>
<td>MGMD Socket Creation/options Set Failed. As a result of this, the MGMD Control packets cannot be sent out on an interface.</td>
</tr>
</tbody>
</table>
### Table 62: IGMP-Proxy Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP-Proxy/MLD-Proxy</td>
<td>MGMD-Proxy Protocol Initialization Failed; Family – xxx.</td>
<td>MGMD-Proxy protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable MGMD-Proxy Protocol.</td>
</tr>
<tr>
<td>IGMP-Proxy/MLD-Proxy</td>
<td>MGMD-Proxy Protocol Heap Memory De-Init Failed; Family – xxx.</td>
<td>MGMD-Proxy Heap memory de-initialization is Failed for the specified address family. This message appears when trying to disable MGMD-Proxy Protocol. As a result of this, the subsequent attempts to enable/disable MGMD-Proxy will also fail.</td>
</tr>
<tr>
<td>IGMP-Proxy/MLD-Proxy</td>
<td>MGMD Proxy Route Entry Creation Failed; grpAddr - xxx, srcAddr – xxx, rtrIfNum – xxx.</td>
<td>Registration of the Multicast Forwarding entry for the specified Source and Group Address Failed when MGMD-Proxy is used.</td>
</tr>
</tbody>
</table>

### Table 63: PIM-SM Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIMSM</td>
<td>Non-Zero SPT/Data Threshold Rate – xxx is currently Not Supported on this platform.</td>
<td>This message appears when the user tries to configure the PIMSM SPT threshold value.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSM Protocol Heap Memory Init Failed; Family – xxx.</td>
<td>PIMSM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMSM Protocol.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSM Protocol Heap Memory De-Init Failed; Family – xxx.</td>
<td>PIMSM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMSM Protocol. As a result of this, the subsequent attempts to enable/disable PIMSM will also fail.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSM Protocol Initialization Failed; Family – xxx.</td>
<td>PIMSM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMSM Protocol.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSM Protocol De-Initialization Failed; Family – xxx.</td>
<td>PIMSM protocol de-initialization sequence Failed. This message appears when trying to disable PIMSM Protocol.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSM SSM Range Table is Full.</td>
<td>PIMSM SSM Range Table is Full. This message appears when the protocol cannot accommodate new SSM registrations.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.</td>
<td>PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.</td>
</tr>
</tbody>
</table>
Table 63: PIM-SM Log Messages (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIMSM</td>
<td>PIM All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.</td>
<td>PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>Mcast Forwarding Mode Disable Failed for intf – xxx.</td>
<td>Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>Mcast Forwarding Mode Enable Failed for intf – xxx.</td>
<td>Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.</td>
<td>PIMSMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.</td>
<td>PIMSMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIM Control packets are still received on the interface at the application though no protocol is enabled.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSM (S,G,RPt) Table Max Limit – xxx Reached; Cannot accommodate any further routes.</td>
<td>PIMSM Multicast Route table (S,G,RPt) has reached maximum capacity and cannot accommodate new registrations anymore.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSM (S,G) Table Max Limit - xxx Reached; Cannot accommodate any further routes.</td>
<td>PIMSM Multicast Route table (S,G) has reached maximum capacity and cannot accommodate new registrations anymore.</td>
</tr>
<tr>
<td>PIMSM</td>
<td>PIMSM (*,G) Table Max Limit - xxx Reached; Cannot accommodate any further routes.</td>
<td>PIMSM Multicast Route table (*.G) has reached maximum capacity and cannot accommodate new registrations anymore.</td>
</tr>
</tbody>
</table>

Table 64: PIM-DM Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIMDM</td>
<td>PIMDM Protocol Heap Memory Init Failed; Family – xxx.</td>
<td>PIMDM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMDM Protocol.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIMDM Protocol Heap Memory De-Init Failed; Family –xxx.</td>
<td>PIMDM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMDM Protocol. As a result of this, the subsequent attempts to enable/disable PIMDM will also fail.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIMDM Protocol Initialization Failed; Family –xxx.</td>
<td>PIMDM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMDM Protocol.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIMDM Protocol De-Initialization Failed; Family – xxx.</td>
<td>PIMDM protocol de-initialization sequence Failed. This message appears when trying to disable PIMDM Protocol.</td>
</tr>
<tr>
<td>Component</td>
<td>Message</td>
<td>Cause</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.</td>
<td>PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIM All Routers Address – xxx Add to the DTL Mcast List Failed for intf – xxx.</td>
<td>PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>Mcast Forwarding Mode Disable Failed for intf – xxx.</td>
<td>Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>Mcast Forwarding Mode Enable Failed for intf – xxx.</td>
<td>Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIMDMv6 Socket Memb'ship Enable Failed for rtrIfNum – xxx.</td>
<td>PIMDMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIMDMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.</td>
<td>PIMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIMv6 packets will not be received by the application.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIMDMv6 Socket Memb'ship Enable Failed for rtrIfNum – xxx.</td>
<td>PIMDMv6 Socket Creation/options Set Failed. As a result of this, the PIM Control packets cannot be sent out on an interface.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIMDMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.</td>
<td>Socket options Set to enable the reception of PMv6 packets Failed. As a result of this, the PMv6 packets will not be received by the application.</td>
</tr>
<tr>
<td>PIMDM</td>
<td>PIMDM MRT Table Max Limit - xxx Reached; Cannot accommodate any further routes.</td>
<td>PIMDM Multicast Route table (S,G) has reached maximum capacity and cannot accommodate new registrations anymore.</td>
</tr>
<tr>
<td>Component</td>
<td>Message</td>
<td>Cause</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>DVMRP</td>
<td>DVMRP Heap memory initialization is Failed for the specified address family.</td>
<td>This message appears when trying to enable DVMRP Protocol.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>DVMRP Heap memory de-initialization is Failed for the specified address family.</td>
<td>This message appears when trying to disable DVMRP Protocol. As a result of this, the subsequent attempts to enable/disable DVMRP will also fail.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>DVMRP protocol initialization sequence Failed.</td>
<td>This could be due to the non-availability of some resources. This message appears when trying to enable DVMRP Protocol.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>DVMRP All Routers Address - xxx Delete from the DTL Mcast List Failed for intf – xxx.</td>
<td>DMVRP All Routers Address deletion from the local multicast list Failed. As a result of this, DVMRP Multicast packets are still received at the application though DVMRP is disabled.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>Mcast Forwarding Mode Disable Failed for intf – xxx.</td>
<td>The Multicast Forwarding mode Disable Failed for this routing interface.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>DVMRP All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.</td>
<td>DMVRP All Routers Address addition to the local multicast list Failed. As a result of this, DVMRP Multicast packets with this address will not be received at the application.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>Mcast Forwarding Mode Enable Failed for intf – xxx.</td>
<td>The Multicast Forwarding mode Enable Failed for this routing interface. As a result of this, the ability to forward Multicast packets does not function on this interface.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>DVMRP Probe Control message Send Failed on rtrIfNum – xxx.</td>
<td>DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>DVMRP Prune Control message Send Failed; rtrIfNum – xxx.</td>
<td>Neighbor - %s, SrcAddr - %s, GrpAddr - %s DVMRP Prune control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the unwanted multicast traffic is still received and forwarded.</td>
</tr>
<tr>
<td>DVMRP</td>
<td>DVMRP Probe Control message Send Failed on rtrIfNum –xxx.</td>
<td>DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.</td>
</tr>
</tbody>
</table>
## 10.8 Technologies

### Table 66: Broadcom Error Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcom</td>
<td>Invalid USP unit = x, slot = x, port = x</td>
<td>A port was not able to be translated correctly during the receive.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x</td>
<td>Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Failed installing mirror action - rest of the policy applied successfully</td>
<td>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.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Policy x does not contain rule x</td>
<td>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.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>ERROR: policy x, tmpPolicy x, size x, data x x x x x x x x x x</td>
<td>An issue installing the policy due to a possible duplicate hash.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>ACL x not found in internal table</td>
<td>Attempting to delete a non-existent ACL.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>ACL internal table overflow</td>
<td>Attempting to add an ACL to a full table.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x</td>
<td>Attempting to configure the bandwidth beyond it's capabilities.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to put sync response on queue</td>
<td>A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync ipmc table on unit = x</td>
<td>Either the transport failed or the message was dropped.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>usl_task_ipmc_msg_send(): failed to send with x</td>
<td>Either the transport failed or the message was dropped.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: No available entries in the STG table</td>
<td>The Spanning Tree Group table is full in USL.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync stg table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: A Trunk doesn't exist in USL</td>
<td>Attempting to modify a Trunk that doesn't exist.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: A Trunk being created by bcmx already existed in USL</td>
<td>Possible synchronization issue between the application, hardware, and sync layer.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: A Trunk being destroyed doesn't exist in USL</td>
<td>Possible synchronization issue between the application, hardware, and sync layer.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: A Trunk being set doesn't exist in USL</td>
<td>Possible synchronization issue between the application, hardware, and sync layer.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync trunk table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: Mcast entry not found on a join</td>
<td>Possible synchronization issue between the application, hardware, and sync layer.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: Mcast entry not found on a leave</td>
<td>Possible synchronization issue between the application, hardware, and sync layer.</td>
</tr>
</tbody>
</table>
Table 66: Broadcom Error Messages (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync dVLAN data on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync policy table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync VLAN table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Invalid LAG id x</td>
<td>Possible synchronization issue between the BCM driver and HAPI.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Invalid uport calculated from the BCM uport</td>
<td>Uport not valid from BCM driver.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Invalid USP calculated from the BCM uport</td>
<td>USP not able to be calculated from the learn event for BCM driver.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Unable to insert route R/P</td>
<td>Route R with prefix P could not be inserted in the hardware route table. A retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Unable to Insert host H</td>
<td>Host H could not be inserted in hardware host table. A retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync L3 Intf table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync L3 Host table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync L3 Route table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync initiator table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync terminator table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
<tr>
<td>Broadcom</td>
<td>USL: failed to sync ip-multicast table on unit = x</td>
<td>Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.</td>
</tr>
</tbody>
</table>
10.9 O/S Support

Table 67: Linux BSP Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux BSP</td>
<td>rc = 10</td>
<td>Second message logged at bootup, right after Starting code... Always logged.</td>
</tr>
</tbody>
</table>

Table 68: OSAPI Linux Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSAPI Linux</td>
<td>osapiNetLinkNeighDump: could not open socket! – or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX</td>
<td>Couldn’t open a netlink socket. Make sure “ARP Daemon support” (CONFIG_ARPD) is enabled in the Linux kernel, if the reference kernel binary is not being used.</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>ipstkNdpFlush: sending delete failed</td>
<td>Failed when telling the kernel to delete a neighbor table entry (the message is incorrect).</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>unable to open /proc/net/ipv6/conf/default/hop_limit</td>
<td>IPv6 MIB objects read, but /proc file system is not mounted, or running kernel does not have IPv6 support.</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ</td>
<td>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.</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: Failed to Delete Route</td>
<td>Error adding or deleting a default gateway in the kernel’s routing table (the function is really osapiRawMRouteAdd()/Delete()).</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: ioctl on XX failed: addr: 0x%YY</td>
<td>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).</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>ping: sendto error</td>
<td>Trouble sending an ICMP echo request packet for the UI ping command. Maybe there was no route to that network.</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>Failed to Create Interface</td>
<td>Out of memory at system initialization time.</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>TAP Unable to open XX</td>
<td>The /dev/tap file is missing, or, if not using the reference kernel binary, the kernel is missing “Universal TUN/TAP device driver support” (CONFIG_TUN).</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX</td>
<td>Trouble reading the /dev/tap device, check the error message XX for details.</td>
</tr>
</tbody>
</table>
Table 68: OSAPI Linux Log Messages (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSAPI Linux</td>
<td>Log_Init: log file error - creating new log file</td>
<td>This pertains to the &quot;event log&quot; persistent file in flash. Either it did not exist, or had a bad checksum.</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>Log_Init: Flash (event) log full; erasing</td>
<td>Event log file has been cleared; happens at boot time.</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>Log_Init: Corrupt event log; erasing</td>
<td>Event log file had a non-blank entry after a blank entry; therefore, something was messed up.</td>
</tr>
<tr>
<td>OSAPI Linux</td>
<td>Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve Interface Flags</td>
<td>Trouble adding VRRP IP or MAC address(es) to a Linux network interface.</td>
</tr>
</tbody>
</table>
APPENDIX A: List of Commands

{deny | permit} (IP ACL) ................................................................. 774
{deny | permit} (IPv6) ................................................................. 785
{deny | permit} (MAC ACL) ............................................................. 763
1583 compatibility ............................................................... 584
aaa accounting ................................................................. 66
aaa authentication dot1x default ................................................ 355
aaa authentication enable .......................................................... 47
aaa authentication login ............................................................ 46
aaa authorization ........................................................................ 48
aaa ias-user username .............................................................. 66
aaa server radius dynamic-author ............................................... 85
aaa session-id ................................................................. 66
absolute .................................................................................. 793
accept-mode ............................................................................. 564
access-list ................................................................................. 769
access-list counters enable ....................................................... 773
accounting ............................................................................... 69
acl-trapflags ........................................................................... 780
acl-traptime ............................................................................. 783
addport ...................................................................................... 390
address .................................................................................... 566
address prefix (IPv6) .............................................................. 716
advertise speed ........................................................................ 296
announce interval ..................................................................... 271
announce timeout ..................................................................... 272
area default-cost (OSPF) ....................................................... 585
area default-cost (OSPFv3) ..................................................... 680
area nssa (OSPF) ...................................................................... 585
area nssa (OSPFv3) .................................................................... 680
area nssa default-info-originate (OSPF) ..................................... 585
area nssa default-info-originate (OSPFv3) .............................. 680
area nssa no-redistribute (OSPF) ........................................... 586
area nssa no-redistribute (OSPFv3) ......................................... 681
area nssa no-summary (OSPF) .................................................. 586
area nssa no-summary (OSPFv3) ............................................... 681
area nssa translator-role (OSPF) ............................................. 586
area nssa translator-role (OSPFv3) ........................................... 681
area nssa translator-stab-intv (OSPF) ....................................... 587
area nssa translator-stab-intv (OSPFv3) .................................... 682
area range (OSPF) ............................................................... 587
area range (OSPFv3) .............................................................. 682
area stub (OSPF) ................................................................. 588
area stub (OSPFv3) ................................................................. 683
area stub no-summary (OSPF) ................................................. 589
area stub no-summary (OSPFv3) ............................................... 683
area virtual-link (OSPF) ......................................................... 589
area virtual-link (OSPFv3) ........................................................ 683
area virtual-link authentication ............................................. 590
area virtual-link dead-interval (OSPF) ..................................... 590
area virtual-link dead-interval (OSPFv3) ................................................................. 684
area virtual-link hello-interval (OSPF) ................................................................. 591
area virtual-link hello-interval (OSPFv3) ................................................................. 684
area virtual-link retransmit-interval (OSPF) ......................................................... 591
area virtual-link retransmit-interval (OSPFv3) ......................................................... 684
area virtual-link transmit-delay (OSPF) ............................................................... 592
area virtual-link transmit-delay (OSPFv3) ............................................................. 685
arp ...................................................................................................................... 509
arp access-list ..................................................................................................... 446
arp cachesize ...................................................................................................... 511
arp dynamicrenew .............................................................................................. 511
arp purge ........................................................................................................... 511
arp resptime ...................................................................................................... 512
arp retries .......................................................................................................... 512
arp timeout ........................................................................................................ 512
assign-queue ..................................................................................................... 750
authentication command bounce-port ignore ..................................................... 85
authentication enable .......................................................................................... 362
authentication order ............................................................................................ 362
authentication priority .......................................................................................... 363
authentication timer restart .................................................................................. 363
authorization commands ..................................................................................... 50
authorization exec ............................................................................................... 50
authorization exec default ................................................................................... 51
authorization network radius .............................................................................. 86
auth-type ........................................................................................................... 86
auto-cost (OSPF) ............................................................................................... 592
auto-cost (OSPFv3) ............................................................................................. 685
auto-negotiate ..................................................................................................... 290
auto-negotiate all ................................................................................................. 290
auto-summary ..................................................................................................... 632
auto-voip ........................................................................................................... 794
auto-voip oui ...................................................................................................... 795
auto-voip oui-based priority ............................................................................... 795
auto-voip protocol-based .................................................................................... 796
auto-voip vlan .................................................................................................... 796
bandwidth .......................................................................................................... 603
cbcmsh ................................................................................................................ 236
bfd ...................................................................................................................... 640
bfd echo ............................................................................................................ 641
bfd interval ....................................................................................................... 641
bfd slow-timer ................................................................................................... 642
block .................................................................................................................. 297
boot autoinstall .................................................................................................. 114
boot host autoreboot ......................................................................................... 115
boot host autosave ............................................................................................. 115
boot host dhcp .................................................................................................. 115
boot host retrycount .......................................................................................... 114
boot system ....................................................................................................... 118
bootfile ............................................................................................................. 181
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootpdhcprelay cidoptmode</td>
<td>573</td>
</tr>
<tr>
<td>bootpdhcprelay enable</td>
<td>575</td>
</tr>
<tr>
<td>bootpdhcprelay maxhopcount</td>
<td>574</td>
</tr>
<tr>
<td>bootpdhcprelay minwaittime</td>
<td>574</td>
</tr>
<tr>
<td>bootpdhcprelay serverip</td>
<td>575</td>
</tr>
<tr>
<td>bridge aging-time</td>
<td>498</td>
</tr>
<tr>
<td>cablestatus</td>
<td>237</td>
</tr>
<tr>
<td>capability opaque</td>
<td>593</td>
</tr>
<tr>
<td>capture file size</td>
<td>196</td>
</tr>
<tr>
<td>capture file</td>
<td>remote</td>
</tr>
<tr>
<td>capture line wrap</td>
<td>196</td>
</tr>
<tr>
<td>capture remote port</td>
<td>196</td>
</tr>
<tr>
<td>capture start</td>
<td>195</td>
</tr>
<tr>
<td>capture stop</td>
<td>195</td>
</tr>
<tr>
<td>class</td>
<td>752</td>
</tr>
<tr>
<td>class-map</td>
<td>743</td>
</tr>
<tr>
<td>class-map rename</td>
<td>743</td>
</tr>
<tr>
<td>classofservice dot1p-mapping</td>
<td>732</td>
</tr>
<tr>
<td>classofservice ip-dscp-mapping</td>
<td>733</td>
</tr>
<tr>
<td>classofservice ip-precedence-mapping</td>
<td>733</td>
</tr>
<tr>
<td>classofservice trust</td>
<td>734</td>
</tr>
<tr>
<td>clear aaa ias-users</td>
<td>68</td>
</tr>
<tr>
<td>clear accounting statistics</td>
<td>70</td>
</tr>
<tr>
<td>clear arp-cache</td>
<td>513</td>
</tr>
<tr>
<td>clear arp-switch</td>
<td>513</td>
</tr>
<tr>
<td>clear authentication authentication-history</td>
<td>366</td>
</tr>
<tr>
<td>clear authentication statistics</td>
<td>366</td>
</tr>
<tr>
<td>clear config</td>
<td>154</td>
</tr>
<tr>
<td>clear config interface</td>
<td>155</td>
</tr>
<tr>
<td>clear counters</td>
<td>155</td>
</tr>
<tr>
<td>clear counters keepalive</td>
<td>325</td>
</tr>
<tr>
<td>clear cpu-traffic</td>
<td>202</td>
</tr>
<tr>
<td>clear dhcp l2relay statistics interface</td>
<td>433</td>
</tr>
<tr>
<td>clear dot1x authentication-history</td>
<td>355</td>
</tr>
<tr>
<td>clear dot1x statistics</td>
<td>355</td>
</tr>
<tr>
<td>clear errcounter</td>
<td>165</td>
</tr>
<tr>
<td>clear host</td>
<td>193</td>
</tr>
<tr>
<td>clear igmpsnoping</td>
<td>155</td>
</tr>
<tr>
<td>clear ip access-list counters</td>
<td>155</td>
</tr>
<tr>
<td>clear ip address-conflict-detect</td>
<td>195</td>
</tr>
<tr>
<td>clear ip arp inspection statistics</td>
<td>448</td>
</tr>
<tr>
<td>clear ip dhcp binding</td>
<td>186</td>
</tr>
<tr>
<td>clear ip dhcp conflict</td>
<td>186</td>
</tr>
<tr>
<td>clear ip dhcp force-client-id</td>
<td>435</td>
</tr>
<tr>
<td>clear ip dhcp force-client-id</td>
<td>457</td>
</tr>
<tr>
<td>clear ip dhcp server statistics</td>
<td>186</td>
</tr>
<tr>
<td>clear ip dhcp snooping binding</td>
<td>442</td>
</tr>
<tr>
<td>clear ip dhcp snooping statistics</td>
<td>442</td>
</tr>
<tr>
<td>clear ip helper statistics</td>
<td>578</td>
</tr>
<tr>
<td>clear ip mroute</td>
<td>811</td>
</tr>
</tbody>
</table>
clear ip ospf .......................................................... 593
clear ip ospf configuration ......................................... 593
clear ip ospf counters ............................................... 593
clear ip ospf neighbor ............................................... 594
clear ip ospf neighbor interface ................................... 594
clear ip ospf redistribution ........................................ 594
clear ip ospf stub-router ........................................... 614
clear ip prefix-list .................................................... 549
clear ip route counters ............................................. 534
clear ipv6 access-list counters .................................... 155
clear ipv6 dhcp ....................................................... 722
clear ipv6 dhcp binding ............................................ 722
clear ipv6 dhcp snooping binding ............................... 729
clear ipv6 dhcp snooping statistics ............................. 729
clear ipv6 mld counters ........................................... 862
clear ipv6 mld traffic ................................................. 862
clear ipv6 mroute .................................................... 845
clear ipv6 neighbors ................................................. 670
clear ipv6 ospf ........................................................ 686
clear ipv6 ospf configuration ..................................... 686
clear ipv6 ospf counters ............................................ 686
clear ipv6 ospf neighbor ............................................ 686
clear ipv6 ospf neighbor interface .............................. 686
clear ipv6 ospf redistribution ..................................... 687
clear ipv6 ospf stub-router ....................................... 701
clear ipv6 prefix-list ............................................... 549
clear ipv6 route counters ........................................ 679
clear ipv6 snooping counters ..................................... 679
clear ipv6 statistics ................................................... 679
clear isdp counters ................................................. 501
clear isdp table ....................................................... 501
clear lldp remote-data .............................................. 477
clear lldp statistics ................................................. 477
clear logging buffered ............................................ 147
clear logging email statistics ..................................... 151
clear mac access-list counters .................................. 155
clear mac-addr-table .............................................. 140
clear mld snooping .................................................. 468
clear network ipv6 dhcp statistics ............................. 722
clear packet-trace packet-data ................................... 235
clear pass ............................................................. 156
clear port-channel all counters .................................. 407
clear port-channel counters ...................................... 407
clear radius dynamic-author statistics ...................... 87
clear radius statistics .............................................. 355
clear serviceport ipv6 dhcp statistics ....................... 723
clear traplog .......................................................... 156
clear vlan ............................................................. 156
clear vpc statistics .................................................. 417
clear vrrp statistics .................................................. 567
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>deleteport (Global Config)</td>
<td>390</td>
</tr>
<tr>
<td>delete</td>
<td>118</td>
</tr>
<tr>
<td>delay-req interval</td>
<td>272</td>
</tr>
<tr>
<td>default-router</td>
<td>179</td>
</tr>
<tr>
<td>default-metric (RIP)</td>
<td>633</td>
</tr>
<tr>
<td>default-metric (OSPFv3)</td>
<td>687</td>
</tr>
<tr>
<td>default-metric (OSPF)</td>
<td>595</td>
</tr>
<tr>
<td>default-information originate (OSPF)</td>
<td>595</td>
</tr>
<tr>
<td>debug vpc peer-link control-message async</td>
<td>417</td>
</tr>
<tr>
<td>debug vpc peer-link control-message bulk</td>
<td>417</td>
</tr>
<tr>
<td>debug vpc peer-link control-message ckpt</td>
<td>417</td>
</tr>
<tr>
<td>debug vpc peer-link data-message</td>
<td>417</td>
</tr>
<tr>
<td>default-information originate (OSPFv3)</td>
<td>595</td>
</tr>
<tr>
<td>default-information originate (OSPFv3)</td>
<td>595</td>
</tr>
<tr>
<td>default-information originate (RIP)</td>
<td>687</td>
</tr>
<tr>
<td>default-metric (OSPF)</td>
<td>95</td>
</tr>
<tr>
<td>default-metric (OSPFv3)</td>
<td>687</td>
</tr>
<tr>
<td>default-metric (RIP)</td>
<td>633</td>
</tr>
<tr>
<td>default-router</td>
<td>179</td>
</tr>
<tr>
<td>delay-req interval</td>
<td>272</td>
</tr>
<tr>
<td>delete</td>
<td>118</td>
</tr>
<tr>
<td>deleteport (Global Config)</td>
<td>390</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>deleteport (Interface Config)</td>
<td>390</td>
</tr>
<tr>
<td>description</td>
<td>291</td>
</tr>
<tr>
<td>dhcp client vendor-id-option</td>
<td>433</td>
</tr>
<tr>
<td>dhcp client vendor-id-option-string</td>
<td>433</td>
</tr>
<tr>
<td>dhcp l2relay</td>
<td>427</td>
</tr>
<tr>
<td>dhcp l2relay circuit-id subscription</td>
<td>428</td>
</tr>
<tr>
<td>dhcp l2relay circuit-id vlan</td>
<td>428</td>
</tr>
<tr>
<td>dhcp l2relay remote-id subscription</td>
<td>428</td>
</tr>
<tr>
<td>dhcp l2relay remote-id vlan</td>
<td>429</td>
</tr>
<tr>
<td>dhcp l2relay subscription</td>
<td>429</td>
</tr>
<tr>
<td>dhcp l2relay trust</td>
<td>429</td>
</tr>
<tr>
<td>dhcp l2relay vlan</td>
<td>430</td>
</tr>
<tr>
<td>diffserv</td>
<td>742</td>
</tr>
<tr>
<td>dir</td>
<td>137</td>
</tr>
<tr>
<td>disconnect</td>
<td>45</td>
</tr>
<tr>
<td>distance ospf (OSPF)</td>
<td>595</td>
</tr>
<tr>
<td>distance ospf (OSPFv3)</td>
<td>687</td>
</tr>
<tr>
<td>distance rip</td>
<td>633</td>
</tr>
<tr>
<td>distribute-list out (OSPF)</td>
<td>596</td>
</tr>
<tr>
<td>distribute-list out (RIP)</td>
<td>633</td>
</tr>
<tr>
<td>dns-server</td>
<td>179</td>
</tr>
<tr>
<td>do (Privileged EXEC commands)</td>
<td>22</td>
</tr>
<tr>
<td>domain-name</td>
<td>181</td>
</tr>
<tr>
<td>domain-name (IPv6)</td>
<td>717</td>
</tr>
<tr>
<td>domain-name enable</td>
<td>182</td>
</tr>
<tr>
<td>dos-control all</td>
<td>488</td>
</tr>
<tr>
<td>dos-control firstfrag</td>
<td>489</td>
</tr>
<tr>
<td>dos-control icmpfrag</td>
<td>496</td>
</tr>
<tr>
<td>dos-control icmpv4</td>
<td>495</td>
</tr>
<tr>
<td>dos-control icmpv6</td>
<td>495</td>
</tr>
<tr>
<td>dos-control l4port</td>
<td>490</td>
</tr>
<tr>
<td>dos-control sipdip</td>
<td>489</td>
</tr>
<tr>
<td>dos-control smacdmac</td>
<td>491</td>
</tr>
<tr>
<td>dos-control tcpfinurgpsh</td>
<td>494</td>
</tr>
<tr>
<td>dos-control tcpflag</td>
<td>490</td>
</tr>
<tr>
<td>dos-control tcpflagseq</td>
<td>492</td>
</tr>
<tr>
<td>dos-control tcpfrag</td>
<td>489</td>
</tr>
<tr>
<td>dos-control tcpoffset</td>
<td>493</td>
</tr>
<tr>
<td>dos-control tcpport</td>
<td>491</td>
</tr>
<tr>
<td>dos-control tcpsyn</td>
<td>493</td>
</tr>
<tr>
<td>dos-control tcpsynfin</td>
<td>494</td>
</tr>
<tr>
<td>dos-control udpport</td>
<td>492</td>
</tr>
<tr>
<td>dot1x dynamic-vlan enable</td>
<td>356</td>
</tr>
<tr>
<td>dot1x eapolflood</td>
<td>356</td>
</tr>
<tr>
<td>dot1x guest-vlan</td>
<td>356</td>
</tr>
<tr>
<td>dot1x initialize</td>
<td>357</td>
</tr>
<tr>
<td>dot1x mac-auth-bypass</td>
<td>359</td>
</tr>
<tr>
<td>dot1x max-req</td>
<td>357</td>
</tr>
<tr>
<td>dot1x max-users</td>
<td>357</td>
</tr>
</tbody>
</table>
dot1x supplicant timeout start-period ........................................... 372
dot1x supplicant timeout held-period ........................................ 373
dot1x supplicant timeout start-period ........................................ 372
dot1x supplicant user ................................................................. 373
dot1x system-auth-control ......................................................... 360
dot1x system-auth-control monitor ............................................. 360
dot1x timeout ............................................................................ 361
dot1x unauthenticated-vlan ....................................................... 361
dot1x user .................................................................................. 362
drop ......................................................................................... 751
dvlan-tunnel ethertype (Interface Config) .................................. 336
dvlan-tunnel ethertype primary-tpid ......................................... 337
enable (OSPF) ........................................................................... 583
enable (OSPFv3) ................................................................. 688
enable (Privileged EXEC access) ............................................. 22
enable (RIP) ............................................................................ 631
enable authentication .............................................................. 52
enable password (Privileged EXEC) ........................................... 60
capsulation ............................................................................. 522
erase factory-defaults .............................................................. 116
erase startup-config ............................................................... 116
errdisable recovery cause ....................................................... 506
errdisable recovery interval .................................................... 506
exception core-file ................................................................. 224
exception dump compression ................................................... 225
exception dump filepath ........................................................ 223
exception dump ftp-server ...................................................... 225
exception dump nfs ............................................................. 223
exception dump stack-ip-address add .................................... 226
exception dump stack-ip-address protocol ............................. 225
exception dump stack-ip-address remove .............................. 226
exception dump tftp-server ..................................................... 222
exception nmi ................................................................. 226
exception protocol ............................................................. 222
exception switch-chip-register ............................................ 224
Exec Authorization ................................................................. 49
exit-overflow-interval (OSPF) ................................................. 596
exit-overflow-interval (OSPFv3) ............................................. 688
external-lsdb-limit (OSPF) .................................................... 597
external-lsdb-limit (OSPFv3) ................................................. 688
feature bfd ................................................................. 640
feature vpc ................................................................. 408
fhrp version vrrp v3 ............................................................. 562
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ssh</td>
<td>34</td>
</tr>
<tr>
<td>ip ssh port</td>
<td>34</td>
</tr>
<tr>
<td>ip ssh protocol</td>
<td>34</td>
</tr>
<tr>
<td>ip ssh server enable</td>
<td>34</td>
</tr>
<tr>
<td>ip telnet port</td>
<td>30</td>
</tr>
<tr>
<td>ip telnet server enable</td>
<td>29</td>
</tr>
<tr>
<td>ip unreachable</td>
<td>638</td>
</tr>
<tr>
<td>ip verify binding</td>
<td>437</td>
</tr>
<tr>
<td>ip verify source</td>
<td>439</td>
</tr>
<tr>
<td>ip vrrp (Global Config)</td>
<td>555</td>
</tr>
<tr>
<td>ip vrrp (Interface Config)</td>
<td>555</td>
</tr>
<tr>
<td>ip vrrp accept-mode</td>
<td>556</td>
</tr>
<tr>
<td>ip vrrp authentication</td>
<td>557</td>
</tr>
<tr>
<td>ip vrrp ip</td>
<td>556</td>
</tr>
<tr>
<td>ip vrrp mode</td>
<td>555</td>
</tr>
<tr>
<td>ip vrrp preempt</td>
<td>557</td>
</tr>
<tr>
<td>ip vrrp priority</td>
<td>558</td>
</tr>
<tr>
<td>ip vrrp timers advertise</td>
<td>558</td>
</tr>
<tr>
<td>ip vrrp track interface</td>
<td>558</td>
</tr>
<tr>
<td>ip vrrp track ip route</td>
<td>559</td>
</tr>
<tr>
<td>ipv6 access-list</td>
<td>784</td>
</tr>
<tr>
<td>ipv6 access-list rename</td>
<td>785</td>
</tr>
<tr>
<td>ipv6 access-list resequence</td>
<td>785</td>
</tr>
<tr>
<td>ipv6 address</td>
<td>654</td>
</tr>
<tr>
<td>ipv6 address autoconfig</td>
<td>654</td>
</tr>
<tr>
<td>ipv6 address dhcp</td>
<td>655</td>
</tr>
<tr>
<td>ipv6 dhcp client pd</td>
<td>714</td>
</tr>
<tr>
<td>ipv6 dhcp pool</td>
<td>716</td>
</tr>
<tr>
<td>ipv6 dhcp relay destination</td>
<td>715</td>
</tr>
<tr>
<td>ipv6 dhcp relay remote-id</td>
<td>715</td>
</tr>
<tr>
<td>ipv6 dhcp server</td>
<td>715</td>
</tr>
<tr>
<td>ipv6 dhcp snooping</td>
<td>723</td>
</tr>
<tr>
<td>ipv6 dhcp snooping binding</td>
<td>724</td>
</tr>
<tr>
<td>ipv6 dhcp snooping database</td>
<td>724</td>
</tr>
<tr>
<td>ipv6 dhcp snooping limit</td>
<td>725</td>
</tr>
<tr>
<td>ipv6 dhcp snooping log-invalid</td>
<td>725</td>
</tr>
<tr>
<td>ipv6 dhcp snooping trust</td>
<td>725</td>
</tr>
<tr>
<td>ipv6 dhcp snooping verify mac-address</td>
<td>723</td>
</tr>
<tr>
<td>ipv6 dhcp snooping vlan</td>
<td>723</td>
</tr>
<tr>
<td>ipv6 enable</td>
<td>653</td>
</tr>
<tr>
<td>ipv6 hop-limit</td>
<td>653</td>
</tr>
<tr>
<td>ipv6 host</td>
<td>192</td>
</tr>
<tr>
<td>ipv6 icmp error-interval</td>
<td>664</td>
</tr>
<tr>
<td>ipv6 mld last-member-query-count</td>
<td>859</td>
</tr>
<tr>
<td>ipv6 mld last-member-query-interval</td>
<td>858</td>
</tr>
<tr>
<td>ipv6 mld query-interval</td>
<td>857</td>
</tr>
<tr>
<td>ipv6 mld query-max-response-time</td>
<td>858</td>
</tr>
<tr>
<td>ipv6 mld router</td>
<td>857</td>
</tr>
<tr>
<td>ipv6 mld version</td>
<td>859</td>
</tr>
<tr>
<td>ipv6 mld-proxy</td>
<td>862</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>ipv6 mld-proxy reset-status</td>
<td>863</td>
</tr>
<tr>
<td>ipv6 mld-proxy unsolicit-rprt-interval</td>
<td>863</td>
</tr>
<tr>
<td>ipv6 mroute</td>
<td>842</td>
</tr>
<tr>
<td>ipv6 mtu</td>
<td>657</td>
</tr>
<tr>
<td>ipv6 nd dad attempts</td>
<td>657</td>
</tr>
<tr>
<td>ipv6 nd managed-config-flag</td>
<td>658</td>
</tr>
<tr>
<td>ipv6 nd ns-interval</td>
<td>658</td>
</tr>
<tr>
<td>ipv6 nd other-config-flag</td>
<td>658</td>
</tr>
<tr>
<td>ipv6 nd prefix</td>
<td>661</td>
</tr>
<tr>
<td>ipv6 nd ra hop-limit unspecified</td>
<td>659</td>
</tr>
<tr>
<td>ipv6 nd ra-lifetime</td>
<td>659</td>
</tr>
<tr>
<td>ipv6 nd reachable-time</td>
<td>660</td>
</tr>
<tr>
<td>ipv6 nd router-preference</td>
<td>660</td>
</tr>
<tr>
<td>ipv6 nd suppress-ra</td>
<td>660</td>
</tr>
<tr>
<td>ipv6 neighbor</td>
<td>661</td>
</tr>
<tr>
<td>ipv6 neighbors dynamicrenew</td>
<td>662</td>
</tr>
<tr>
<td>ipv6 nud</td>
<td>662</td>
</tr>
<tr>
<td>ipv6 ospf area</td>
<td>693</td>
</tr>
<tr>
<td>ipv6 ospf cost</td>
<td>693</td>
</tr>
<tr>
<td>ipv6 ospf dead-interval</td>
<td>694</td>
</tr>
<tr>
<td>ipv6 ospf hello-interval</td>
<td>694</td>
</tr>
<tr>
<td>ipv6 ospf link-lsa-suppression</td>
<td>695</td>
</tr>
<tr>
<td>ipv6 ospf mtu-ignore</td>
<td>695</td>
</tr>
<tr>
<td>ipv6 ospf network</td>
<td>695</td>
</tr>
<tr>
<td>ipv6 ospf prefix-suppression</td>
<td>696</td>
</tr>
<tr>
<td>ipv6 ospf priority</td>
<td>696</td>
</tr>
<tr>
<td>ipv6 ospf retransmit-interval</td>
<td>697</td>
</tr>
<tr>
<td>ipv6 ospf transmit-delay</td>
<td>697</td>
</tr>
<tr>
<td>ipv6 pim</td>
<td>846</td>
</tr>
<tr>
<td>ipv6 pim bsr-border</td>
<td>847</td>
</tr>
<tr>
<td>ipv6 pim bsr-candidate</td>
<td>848</td>
</tr>
<tr>
<td>ipv6 pim dense</td>
<td>845</td>
</tr>
<tr>
<td>ipv6 pim dr-priority</td>
<td>849</td>
</tr>
<tr>
<td>ipv6 pim hello-interval</td>
<td>847</td>
</tr>
<tr>
<td>ipv6 pim join-prune-interval</td>
<td>849</td>
</tr>
<tr>
<td>ipv6 pim rp-address</td>
<td>850</td>
</tr>
<tr>
<td>ipv6 pim rp-candidate</td>
<td>850</td>
</tr>
<tr>
<td>ipv6 pim sparse</td>
<td>846</td>
</tr>
<tr>
<td>ipv6 pim ssm</td>
<td>851</td>
</tr>
<tr>
<td>ipv6 prefix-list</td>
<td>537</td>
</tr>
<tr>
<td>ipv6 prefix-list</td>
<td>663</td>
</tr>
<tr>
<td>ipv6 redirects</td>
<td>638</td>
</tr>
<tr>
<td>ipv6 route</td>
<td>655</td>
</tr>
<tr>
<td>ipv6 route distance</td>
<td>656</td>
</tr>
<tr>
<td>ipv6 route net-prototype</td>
<td>656</td>
</tr>
<tr>
<td>ipv6 router ospf</td>
<td>680</td>
</tr>
<tr>
<td>ipv6 traffic-filter</td>
<td>789</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>653</td>
</tr>
<tr>
<td>ipv6 unreachable</td>
<td>664</td>
</tr>
<tr>
<td>ipv6 unresolved-traffic</td>
<td>664</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>ipv6 verify binding</td>
<td>726</td>
</tr>
<tr>
<td>ipv6 verify source</td>
<td>726</td>
</tr>
<tr>
<td>iscsi aging time</td>
<td>798</td>
</tr>
<tr>
<td>iscsi cos</td>
<td>799</td>
</tr>
<tr>
<td>iscsi enable</td>
<td>799</td>
</tr>
<tr>
<td>iscsi target port</td>
<td>800</td>
</tr>
<tr>
<td>isdp advertise-v2</td>
<td>500</td>
</tr>
<tr>
<td>isdp enable</td>
<td>500</td>
</tr>
<tr>
<td>isdp holdtime</td>
<td>500</td>
</tr>
<tr>
<td>isdp run</td>
<td>499</td>
</tr>
<tr>
<td>isdp timer</td>
<td>500</td>
</tr>
<tr>
<td>keepalive (Global Config)</td>
<td>322</td>
</tr>
<tr>
<td>keepalive (Interface Config)</td>
<td>323</td>
</tr>
<tr>
<td>keepalive action</td>
<td>323</td>
</tr>
<tr>
<td>keepalive disable-timer</td>
<td>323</td>
</tr>
<tr>
<td>keepalive retry</td>
<td>324</td>
</tr>
<tr>
<td>key</td>
<td>107</td>
</tr>
<tr>
<td>keystring</td>
<td>107</td>
</tr>
<tr>
<td>L2-port-bridge</td>
<td>508</td>
</tr>
<tr>
<td>lacp actor admin key</td>
<td>391</td>
</tr>
<tr>
<td>lacp actor admin state</td>
<td>393</td>
</tr>
<tr>
<td>lacp actor admin state individual</td>
<td>392</td>
</tr>
<tr>
<td>lacp actor admin state longtimeout</td>
<td>392</td>
</tr>
<tr>
<td>lacp actor admin state passive</td>
<td>393</td>
</tr>
<tr>
<td>lacp actor port priority</td>
<td>393</td>
</tr>
<tr>
<td>lacp admin key</td>
<td>391</td>
</tr>
<tr>
<td>lacp collector max-delay</td>
<td>391</td>
</tr>
<tr>
<td>lacp partner admin key</td>
<td>394</td>
</tr>
<tr>
<td>lacp partner admin state individual</td>
<td>394</td>
</tr>
<tr>
<td>lacp partner admin state longtimeout</td>
<td>395</td>
</tr>
<tr>
<td>lacp partner admin state passive</td>
<td>395</td>
</tr>
<tr>
<td>lacp partner port id</td>
<td>395</td>
</tr>
<tr>
<td>lacp partner port priority</td>
<td>396</td>
</tr>
<tr>
<td>lacp partner system priority</td>
<td>397</td>
</tr>
<tr>
<td>lacp partner system-id</td>
<td>396</td>
</tr>
<tr>
<td>lease</td>
<td>396</td>
</tr>
<tr>
<td>length value</td>
<td>180</td>
</tr>
<tr>
<td>line</td>
<td>139</td>
</tr>
<tr>
<td>link state group</td>
<td>28</td>
</tr>
<tr>
<td>link state group downsteam</td>
<td>382</td>
</tr>
<tr>
<td>link state group upstream</td>
<td>383</td>
</tr>
<tr>
<td>linuxsh</td>
<td>45</td>
</tr>
<tr>
<td>lldp med</td>
<td>481</td>
</tr>
<tr>
<td>lldp med all</td>
<td>482</td>
</tr>
<tr>
<td>lldp med confignotification</td>
<td>481</td>
</tr>
<tr>
<td>lldp med confignotification all</td>
<td>482</td>
</tr>
<tr>
<td>lldp med faststartrepeatecount</td>
<td>483</td>
</tr>
<tr>
<td>lldp med transmit-tlv</td>
<td>482</td>
</tr>
<tr>
<td>lldp med transmit-tlv all</td>
<td>483</td>
</tr>
<tr>
<td>lldp notification</td>
<td>476</td>
</tr>
</tbody>
</table>
lldp notification-interval ................................................................. 476
lldp receive .................................................................................... 475
lldp timers ........................................................................................ 475
lldp transmit .................................................................................. 474
lldp transmit-mgmt ........................................................................ 476
lldp transmit-tlv ............................................................................ 475
lpf ...................................................................................................... 384
local-priority .................................................................................. 270
log-adjacency-changes ................................................................. 597
logging buffered ............................................................................ 140
logging buffered wrap .................................................................... 141
logging cli-command ...................................................................... 141
logging console ............................................................................. 141
logging email ................................................................................. 147
logging email from-addr .............................................................. 148
logging email logtime ................................................................. 149
logging email message-type subject .............................................. 149
logging email message-type to-addr .............................................. 148
logging email test message-type .................................................. 150
logging email urgent ..................................................................... 148
logging host .................................................................................. 142
logging host reconfigure ............................................................. 142
logging host remove ..................................................................... 143
logging persistent .......................................................................... 228
logging protocol ........................................................................... 143
logging syslog ............................................................................... 143
logging syslog port ....................................................................... 143
logging syslog source-interface .................................................. 144
logging traps ................................................................................ 149
login authentication ....................................................................... 58
logout ............................................................................................ 156
mac access-group ......................................................................... 765
mac access-list extended ............................................................ 762
mac access-list extended rename .................................................. 763
mac access-list resequence ......................................................... 763
macfilter ....................................................................................... 424
macfilter adddest ......................................................................... 425
macfilter adddest all ..................................................................... 425
macfilter addsrc .......................................................................... 426
macfilter addsrc all ..................................................................... 426
mac-learn ....................................................................................... 297
mail-server ................................................................................... 151
mark cos ....................................................................................... 752
mark cos-as-sec-cos ..................................................................... 753
mark ip-dscp ............................................................................... 753
mark ip-precedence ....................................................................... 753
mark secondary-cos ..................................................................... 752
match any ...................................................................................... 744
match class-map .......................................................................... 744
netbios-node-type .......................................................... 183
network (DHCP Pool Config) ........................................... 181
network area (OSPF) ..................................................... 584
network ipv6 address .................................................. 647
network ipv6 enable ..................................................... 645
network ipv6 gateway ................................................. 647
network ipv6 neighbor ................................................ 648
network javamode ....................................................... 25
network mac-address .................................................. 24
network mac-type ....................................................... 25
network mgmt_vlan ..................................................... 325
network parms ............................................................ 24
network protocol ....................................................... 24
network protocol dhcp ................................................. 24
next-server ............................................................... 183
no 1583compatibility ................................................... 585
no aaa accounting ...................................................... 68
no aaa authentication enable ....................................... 48
no aaa authentication login ......................................... 47
no aaa authorization .................................................. 50
no aaa ias-user username ............................................ 66
no aaa server radius dynamic-author ......................... 85
no aaa session-id ...................................................... 66
no absolute ............................................................... 793
no accept-mode ........................................................ 564
no access-list ............................................................ 773
no access-list counters enable ...................................... 773
no accounting ........................................................... 70
no acl-trapflags ........................................................ 780
no acl-traptime ........................................................ 784
no address ............................................................... 566
no advertise speed ..................................................... 296
no announce interval .................................................. 272
no announce timeout .................................................. 272
no area nssa .............................................................. 585
no area nssa .............................................................. 680
no area nssa default-info-originate (OSPF) .................. 586
no area nssa default-info-originate (OSPFv3) ............... 681
no area nssa no-redistribute (OSPF) ......................... 586
no area nssa no-redistribute (OSPFv3) ....................... 681
no area nssa no-summary (OSPF) .................... 586
no area nssa no-summary (OSPFv3) ............................ 681
no area nssa translator-role (OSPF) ......................... 587
no area nssa translator-role (OSPFv3) ....................... 682
no area nssa translator-stab-intv (OSPF) .................... 587
no area nssa translator-stab-intv (OSPFv3) ................. 682
no area range ........................................................... 588
no area range ........................................................... 683
no area stub ............................................................. 589
no area stub ............................................................. 683
no bootfile .................................................................................................................. 181
no bootpdhcprelay cidoptmode .............................................................. 574
no bootpdhcprelay enable ............................................................................. 576
no bootpdhcprelay maxhopcount ............................................................. 574
no bootpdhcprelay minwaittime ................................................................. 575
no bootpdhcprelay serverip ......................................................................... 575
no bridge aging-time ...................................................................................... 498
no capability opaque ...................................................................................... 593
no capture line wrap ...................................................................................... 197
no class ............................................................................................................ 752
no class-map ................................................................................................... 744
no classofservice dot1p-mapping ............................................................... 733
no classofservice ip-dscp-mapping ............................................................. 733
no classofservice ip-precedence-mapping ................................................ 734
no classofservice trust ............................................................................... 734
no client ........................................................................................................... 87
no client-identifier ......................................................................................... 179
no client-name ............................................................................................... 179
no clock summer-time .................................................................................. 176
no clock timezone ......................................................................................... 177
no clock-port ................................................................................................. 271
no cos-queue max-bandwidth ....................................................................... 735
no cos-queue min-bandwidth ....................................................................... 735
no cos-queue random-detect ....................................................................... 736
no cos-queue strict ......................................................................................... 736
no cpu-traffic direction interface ................................................................ 197
no cpu-traffic direction match cust-filter .................................................. 198
no cpu-traffic direction match dstip ............................................................ 199
no cpu-traffic direction match srcip ............................................................. 198
no cpu-traffic direction match tcp ................................................................. 199
no cpu-traffic direction match udp ................................................................. 199
no cpu-traffic mode ....................................................................................... 200
no cpu-traffic trace ....................................................................................... 200
no crypto certificate generate ...................................................................... 37
no crypto key generate dsa .......................................................................... 37
no crypto key generate rsa .......................................................................... 37
no dampening ................................................................................................. 610
no debug aaa accounting ............................................................................. 202
no debug aaa authorization ........................................................................ 203
no debug arp ................................................................................................. 203
no debug auto-voip ....................................................................................... 204
no debug console .......................................................................................... 204
no debug dhcp ............................................................................................... 206
no debug dot1x packet .................................................................................. 206
no debug fip-snooping packet ..................................................................... 207
no debug igmsnooping packet .................................................................... 207
no debug igmsnooping receive .................................................................... 209
no debug igmsnooping transmit ................................................................. 208
no debug ip acl .............................................................................................. 209
no debug ip dvmrp packet ........................................................................... 210
no debug ip igmp packet ................................................................. 210
no debug ip mcache packet .......................................................... 210
no debug ip pimdm packet ............................................................. 211
no debug ip pimsm packet ............................................................. 211
no debug ip vrrp ........................................................................... 211
no debug ipv6 dhcp ........................................................................ 212
no debug ipv6 mcache packet ........................................................ 212
no debug ipv6 mld packet .............................................................. 212
no debug ipv6 ospf3 packet ............................................................ 213
no debug ipv6 pimdm packet ........................................................ 213
no debug ipv6 pimsm packet ........................................................ 213
no debug isdp packet ................................................................... 505
no debug lacp packet .................................................................... 214
no debug mldsnooping packet ......................................................... 214
no debug mvr packet .................................................................... 389
no debug mvr trace ....................................................................... 389
no debug ospf packet ..................................................................... 216
no debug ospfv3 packet .................................................................. 216
no debug ping packet ..................................................................... 217
no debug rip packet ........................................................................ 218
no debug sflow packet ................................................................... 218
no debug spanning-tree bpdus ......................................................... 218
no debug spanning-tree bpdus receive .............................................. 219
no debug spanning-tree bpdus transmit .......................................... 220
no debug transfer .......................................................................... 221
no default-information originate (OSPF) .......................................... 595
no default-information originate (OSPFv3) ...................................... 687
no default-information originate (RIP) ............................................. 633
no default-metric (OSPF) ............................................................... 595
no default-metric (OSPFv3) ............................................................. 687
no default-metric (RIP) ................................................................. 633
no default-router ........................................................................... 179
no delay-req interval ...................................................................... 272
no dhcp client vendor-id-option ..................................................... 433
no dhcp client vendor-id-option-string .......................................... 434
no dhcp l2relay ............................................................................ 427
no dhcp l2relay circuit-id subscription ............................................ 428
no dhcp l2relay circuit-id vlan ........................................................ 428
no dhcp l2relay remote-id subscription ........................................... 429
no dhcp l2relay remote-id vlan ....................................................... 429
no dhcp l2relay subscription .......................................................... 429
no dhcp l2relay trust ....................................................................... 430
no dhcp l2relay vlan ....................................................................... 430
no diffserv ..................................................................................... 743
no distance ospf .......................................................................... 596
no distance ospf .......................................................................... 688
no distance rip ............................................................................... 633
no distribute-list out ...................................................................... 596
no distribute-list out ...................................................................... 634
no dns-server ................................................................................ 180
no dns-server .................................................................................................................. 717
no domain-name ........................................................................................................... 182
no domain-name enable .............................................................................................. 182
no dos-control all ........................................................................................................ 489
no dos-control firstfrag ............................................................................................ 489
no dos-control icmpfrag ............................................................................................. 496
no dos-control icmpv4 ............................................................................................... 495
no dos-control icmpv6 ............................................................................................... 496
no dos-control l4port .................................................................................................. 491
no dos-control sipdip ................................................................................................. 489
no dos-control smacdmac ........................................................................................ 491
no dos-control tcpfinurgpsh .................................................................................... 495
no dos-control tcpflag .............................................................................................. 490
no dos-control tcpflags eq ....................................................................................... 493
no dos-control tcpfrag ............................................................................................. 490
no dos-control tcpoffset ........................................................................................... 493
no dos-control tcpport ............................................................................................... 492
no dos-control tcpsyn ............................................................................................... 494
no dos-control tcpsynfin .......................................................................................... 494
no dos-control udpport ............................................................................................. 492
no dot1x dynamic-vlan enable .................................................................................. 356
no dot1x eapolflood ................................................................................................. 356
no dot1x guest-vlan ................................................................................................. 357
no dot1x mac-auth-bypass ....................................................................................... 359
no dot1x max-req ....................................................................................................... 357
no dot1x max-users ................................................................................................. 358
no dot1x port-control ............................................................................................... 358
no dot1x port-control all ........................................................................................ 359
no dot1x re-authentication ....................................................................................... 360
no dot1x supplicant max-start ............................................................................... 372
no dot1x supplicant port-control ............................................................................ 372
no dot1x supplicant timeout auth-period ............................................................... 373
no dot1x supplicant timeout held-period ............................................................... 373
no dot1x supplicant timeout start-period ............................................................... 373
no dot1x system-auth-control ................................................................................ 360
no dot1x system-auth-control monitor ................................................................. 360
no dot1x timeout ....................................................................................................... 361
no dot1x unauthenticated-vlan ............................................................................... 362
no dot1x user .............................................................................................................. 362
no dvlan-tunnel ethertype (Interface Config) .......................................................... 337
no dvlan-tunnel ethertype primary-tpid ................................................................. 337
no enable (OSPF) ..................................................................................................... 584
no enable (OSPFv3) ................................................................................................. 688
no enable (RIP) ........................................................................................................ 632
no enable authentication ........................................................................................ 52
no enable password (Privileged EXEC) ..................................................................... 61
no errdisable recovery cause ................................................................................ 506
no errdisable recovery interval ............................................................................... 506
no exception core-file ............................................................................................ 224
no exception dump compression ................................................................. 225
no exception dump filepath .................................................................... 224
no exception dump ftp-server ................................................................. 225
no exception dump nfs ............................................................................ 223
no exception dump stack-ip-address protocol ........................................ 226
no exception dump tftp-server ................................................................. 223
no exception protocol ............................................................................ 222
no exit-overflow-interval .......................................................... 597, 688
no external-lsdb-limit .............................................................................. 597
no external-lsdb-limit .............................................................................. 689
no feature bfd ......................................................................................... 641
no feature vpc ......................................................................................... 408
no fhrp version vrrp v3 ........................................................................... 562
no file verify .......................................................................................... 166
no flowcontrol ....................................................................................... 348
no flowcontrol {symmetric | asymmetric} ................................................ 347
no hardware-address ............................................................................ 180
no host .................................................................................................. 180
no hostresaccept .................................................................................... 635
no ignore server-key ............................................................................. 88
no ignore session-key .......................................................................... 89
no interface loopback .......................................................................... 652
no interface tunnel ................................................................................. 651
no ip access-group ............................................................................... 780
no ip access-list .................................................................................... 774
no ip address .......................................................... 516, 517, 518, 519
no ip address dhcp ................................................................................ 516
no ip arp inspection filter ..................................................................... 446
no ip arp inspection limit ..................................................................... 445
no ip arp inspection trust ..................................................................... 445
no ip arp inspection validate ............................................................... 444
no ip arp inspection vlan ................................................................... 444
no ip arp inspection vlan logging ......................................................... 445
no ip default-gateway .......................................................................... 517
no ip dhcp bootp automatic ................................................................. 185
no ip dhcp conflict logging .................................................................. 186
no ip dhcp excluded-address ............................................................... 184
no ip dhcp filtering trust ..................................................................... 437
no ip dhcp force-client-id .................................................................... 434
no ip dhcp force-client-id .................................................................... 457
no ip dhcp option-61 ............................................................................. 189
no ip dhcp ping packets ..................................................................... 435
no ip dhcp pool ..................................................................................... 178
no ip dhcp snooping ............................................................................ 435
no ip dhcp snooping binding ................................................................. 437
no ip dhcp snooping database write-delay ........................................... 437
no ip dhcp snooping database write-delay ........................................... 724
no ip dhcp snooping limit .................................................................... 438
no ip dhcp snooping log-invalid ......................................................... 438
no ipv6 nd managed-config-flag ............................................................................. 658
no ipv6 nd dad attempts ................................................................................................. 658
no ipv6 mtu .................................................................................................................. 657
no ipv6 mroute .............................................................................................................. 843
no ipv6 mld-proxy unsolicited-report-interval ..................................................................... 863
no ipv6 mld-proxy .......................................................................................................... 863
no ipv6 mld version ........................................................................................................ 859
no ipv6 mld router ......................................................................................................... 857
no ipv6 mld last-member-query-interval ............................................................................. 858
no ipv6 mld last-member-query-count ............................................................................. 859
no ipv6 mld query-max-response-time ............................................................................ 858
no ipv6 mld query-interval ............................................................................................... 858
no ipv6 mld last-member-query-count ............................................................................. 859
no ipv6 mld query-max-response-time ............................................................................ 858
no ipv6 mld query-interval ............................................................................................... 858
no ipv6 mld version ........................................................................................................ 859
no ipv6 mld-proxy .......................................................................................................... 863
no ipv6 mld-proxy unsolicited-report-interval ..................................................................... 863
no ipv6 mroute .................................................................................................................. 843
no ipv6 mtu .................................................................................................................. 657
no ipv6 nd dad attempts ................................................................................................. 658
no ipv6 nd managed-config-flag .................................................................................... 658
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>no keepalive</td>
<td>323</td>
</tr>
<tr>
<td>no keepalive</td>
<td>323</td>
</tr>
<tr>
<td>no keepalive action</td>
<td>323</td>
</tr>
<tr>
<td>no keepalive disable-timer</td>
<td>324</td>
</tr>
<tr>
<td>no L2-port-bridge</td>
<td>508</td>
</tr>
<tr>
<td>no lacp actor admin key</td>
<td>392</td>
</tr>
<tr>
<td>no lacp actor admin state</td>
<td>393</td>
</tr>
<tr>
<td>no lacp actor admin state individual</td>
<td>392</td>
</tr>
<tr>
<td>no lacp actor admin state longtimeout</td>
<td>392</td>
</tr>
<tr>
<td>no lacp actor admin state passive</td>
<td>393</td>
</tr>
<tr>
<td>no lacp actor port priority</td>
<td>394</td>
</tr>
<tr>
<td>no lacp admin key</td>
<td>391</td>
</tr>
<tr>
<td>no lacp collector max delay</td>
<td>391</td>
</tr>
<tr>
<td>no lacp partner admin key</td>
<td>394</td>
</tr>
<tr>
<td>no lacp partner admin state individual</td>
<td>395</td>
</tr>
<tr>
<td>no lacp partner admin state longtimeout</td>
<td>395</td>
</tr>
<tr>
<td>no lacp partner admin state passive</td>
<td>395</td>
</tr>
<tr>
<td>no lacp partner port id</td>
<td>396</td>
</tr>
<tr>
<td>no lacp partner port priority</td>
<td>396</td>
</tr>
<tr>
<td>no lacp partner system priority</td>
<td>397</td>
</tr>
<tr>
<td>no lacp partner system-id</td>
<td>397</td>
</tr>
<tr>
<td>no ldp med confignotification</td>
<td>482</td>
</tr>
<tr>
<td>no lease</td>
<td>181</td>
</tr>
<tr>
<td>no length value</td>
<td>139</td>
</tr>
<tr>
<td>no link state group</td>
<td>382</td>
</tr>
<tr>
<td>no link state group downsteam</td>
<td>383</td>
</tr>
<tr>
<td>no link state group upstream</td>
<td>383</td>
</tr>
<tr>
<td>no link state track</td>
<td>382</td>
</tr>
<tr>
<td>no ldp med</td>
<td>481</td>
</tr>
<tr>
<td>no ldp med faststartrepeatcount</td>
<td>483</td>
</tr>
<tr>
<td>no ldp med transmit-tlv</td>
<td>482</td>
</tr>
<tr>
<td>no ldp med transmit-tlv</td>
<td>483</td>
</tr>
<tr>
<td>no ldp notification</td>
<td>476</td>
</tr>
<tr>
<td>no ldp notification-interval</td>
<td>477</td>
</tr>
<tr>
<td>no ldp receive</td>
<td>475</td>
</tr>
<tr>
<td>no ldp timers</td>
<td>475</td>
</tr>
<tr>
<td>no ldp transmit</td>
<td>475</td>
</tr>
<tr>
<td>no ldp transmit-mgmt</td>
<td>476</td>
</tr>
<tr>
<td>no ldp transmit-tlv</td>
<td>476</td>
</tr>
<tr>
<td>no llpf</td>
<td>384</td>
</tr>
<tr>
<td>no local-priority</td>
<td>271</td>
</tr>
<tr>
<td>no local-priority</td>
<td>273</td>
</tr>
<tr>
<td>no log-adjacency-changes</td>
<td>598</td>
</tr>
<tr>
<td>no logging buffered</td>
<td>141</td>
</tr>
<tr>
<td>no logging buffered wrap</td>
<td>141</td>
</tr>
<tr>
<td>no logging cli-command</td>
<td>141</td>
</tr>
<tr>
<td>no logging console</td>
<td>142</td>
</tr>
<tr>
<td>no logging email</td>
<td>148</td>
</tr>
<tr>
<td>no logging email from-addr</td>
<td>149</td>
</tr>
<tr>
<td>no logging email logtime</td>
<td>149</td>
</tr>
</tbody>
</table>
no network ipv6 address ................................................................. 647
no network ipv6 enable ................................................................. 645
no network ipv6 gateway .............................................................. 648
no network ipv6 neighbor .............................................................. 648
no network javemode ................................................................. 25
no network mac-type ................................................................. 25
no network mgmt_vlan ............................................................... 325
no next-server ............................................................................... 183
no nsf ......................................................................................... 612
no nsf (OSPFv3) ......................................................................... 698
no nsf [ietf] helper strict-lsa-checking ......................................... 613
no nsf [ietf] helper strict-lsa-checking (OSPFv3) ......................... 700
no nsf helper ............................................................................... 612
no nsf helper (OSPFv3) ............................................................... 699
no nsf-restart-interval ................................................................. 612
no nsf-restart-interval (OSPFv3) .................................................. 698
no option .................................................................................. 184
no passive-interface ..................................................................... 601
no passive-interface ................................................................. 600
no passive-interface default ...................................................... 689
no password (aaa IAS User Config) ............................................. 60
no password (AAA IAS User Configuration) .................................. 68
no password (Line Configuration) ................................................ 59
no passwords aging .................................................................... 62
no passwords history .................................................................... 61
no passwords lock-out ................................................................... 62
no passwords min-length ........................................................... 61
no passwords strength exclude-keyword ........................................ 61
no passwords strength minimum character-classes ...................... 65
no passwords strength minimum lowercase-letters ....................... 63
no passwords strength minimum numeric-characters .................... 64
no passwords strength minimum special-characters ..................... 64
no passwords strength minimum uppercase-letters ....................... 63
no passwords strength-check ...................................................... 62
no peer detection enable .............................................................. 408
no peer detection interval ......................................................... 409
no peer-keepalive destination ..................................................... 409
no peer-keepalive enable ............................................................ 409
no peer-keepalive timeout .......................................................... 409
no periodic .................................................................................. 410
no permit ip host mac host ........................................................... 447
no poe high-power ....................................................................... 282
no poe power management .......................................................... 284
no poe priority ............................................................................ 284
no poe usagethreshold ................................................................. 286
no policy-map .............................................................................. 755
no port ........................................................................................ 89
no port lacpmode ......................................................................... 398
no port lacpmode enable all ......................................................... 398
no rmon event .............................................................................................................. 253
no rmon hcalarm ........................................................................................................... 252
no role priority ............................................................................................................ 410
no route-map .............................................................................................................. 539
no routing .................................................................................................................... 515
no sdm prefer ............................................................................................................. 248
no sequence-number .................................................................................................. 765
no sequence-number .................................................................................................. 779
no sequence-number .................................................................................................. 789
no serial baudrate ....................................................................................................... 28
no serial timeout ......................................................................................................... 29
no server-key .............................................................................................................. 96
no service dhcp ............................................................................................................ 185
no service dhcpv6 ....................................................................................................... 714
no service-policy ......................................................................................................... 757
no serviceport ipv6 address ......................................................................................... 646
no serviceport ipv6 enable .......................................................................................... 645
no serviceport ipv6 gateway ......................................................................................... 646
no serviceport ipv6 neighbor ....................................................................................... 647
no session-limit .......................................................................................................... 31
no session-timeout ....................................................................................................... 32
no set board port-map ................................................................................................ 163
no set board sensor .................................................................................................... 166
no set bootstopkey ...................................................................................................... 162
no set bpdu forwarding ............................................................................................... 407
no set chkconfig ......................................................................................................... 169
no set clibanner ......................................................................................................... 112
no set garp timer join ................................................................................................. 350
no set garp timer leave .............................................................................................. 351
no set garp timer leaveall .......................................................................................... 351
no set gmrp adminmode .............................................................................................. 353
no set gmrp interfacemode .......................................................................................... 354
no set groupmembership-interval ............................................................................... 463
no set gvrp adminmode .............................................................................................. 352
no set gvrp interfacemode .......................................................................................... 352
no set igmp ................................................................................................................ 450
no set igmp fast-leave ................................................................................................. 451
no set igmp groupmembership-interval ...................................................................... 452
no set igmp header-validation .................................................................................... 450
no set igmp interfacemode .......................................................................................... 451
no set igmp maxresponse ............................................................................................ 452
no set igmp mcrtrexpiretime ....................................................................................... 453
no set igmp mrouter .................................................................................................... 453
no set igmp mrouter interface ...................................................................................... 453
no set igmp querier ...................................................................................................... 458
no set igmp querier election participate ..................................................................... 459
no set igmp querier query-interval ............................................................................. 458
no set igmp querier timer expiry ............................................................................... 459
no set igmp querier version ....................................................................................... 459
no set igmp report-suppression ................................................................................ 454
no set ip default next-hop ............................................................... 545
no set ip next-hop ............................................................................. 545
no set ip precedence ........................................................................ 546
no set mld .......................................................................................... 461
no set mld fast-leave ......................................................................... 462
no set mld interfacemode ................................................................. 461
no set mld maxresponse .................................................................... 463
no set mld mcrtexpiretime ................................................................. 464
no set mld mrouter ............................................................................. 464
no set mld mrouter interface ............................................................ 464
no set mld querier ............................................................................. 468
no set mld querier election participate ............................................. 469
no set mld querier query_interval ..................................................... 469
no set mld querier timer expiry ........................................................ 469
no sflow poller .................................................................................. 238
no sflow receiver ............................................................................... 239
no sflow remote-agent ip ................................................................. 240
no sflow remote-agent monitor-session .......................................... 240
no sflow remote-agent port ............................................................. 241
no sflow sample rate ....................................................................... 242
no sflow sampler ............................................................................. 241
no sflow sampler filter ip access-group .......................................... 242
no sflow sampler filter mac access-group ....................................... 243
no sflow sampler remote-agent ....................................................... 242
no sflow source-interface ................................................................. 243
no sfp auto-configure ....................................................................... 167
no sfp auto-isolate ........................................................................... 167
no sfp protocol .................................................................................. 167
no show debugging ........................................................................... 222
no shutdown ..................................................................................... 292
no shutdown all ................................................................................ 293
no set ip precedence ........................................................................ 546
no snmp trap link-status .................................................................... 74
no snmp trap link-status all .............................................................. 74
no snmp-server community ............................................................... 72
no snmp-server enable traps ............................................................. 73
no snmp-server enable traps linkmode .............................................. 75
no snmp-server enable traps multiusers .......................................... 75
no snmp-server enable traps sfp ......................................................... 168
no snmp-server enable traps stpmode .............................................. 76
no snmp-server enable traps violation .............................................. 73
no snmp-server enable traps vrrp ....................................................... 563
no snmp-server engineID local .......................................................... 76
no snmp-server filter ....................................................................... 77
no snmp-server group ...................................................................... 78
no snmp-server host .......................................................................... 78
no snmp-server port ......................................................................... 74
no snmp-server user .......................................................................... 79
no snmp-server view ......................................................................... 80
no snmp-sever enable traps .............................................................. 73
no snmptrap source-interface ................................................................. 81
no snntp broadcast client poll-interval .................................................. 170
no snntp client mode ............................................................................ 170
no snntp client port .............................................................................. 170
no snntp multicast client poll-interval .................................................. 171
no snntp server ..................................................................................... 172
no snntp source-interface ................................................................ 173
no snntp unicast client poll-interval ...................................................... 171
no snntp unicast client poll-retry ........................................................... 172
no snntp unicast client poll-timeout ....................................................... 171
no spanning-tree .................................................................................. 298
no spanning-tree auto-edge .................................................................. 299
no spanning-tree backbonefast .............................................................. 300
no spanning-tree bpdufilter .................................................................. 300
no spanning-tree bpdufilter default ......................................................... 300
no spanning-tree bpduloflood ................................................................. 301
no spanning-tree bpduguard .................................................................. 301
no spanning-tree configuration name ..................................................... 302
no spanning-tree configuration revision ............................................... 302
no spanning-tree cost ........................................................................... 302
no spanning-tree edgeport .................................................................... 303
no spanning-tree forceversion ............................................................... 303
no spanning-tree forward-time .............................................................. 303
no spanning-tree guard ......................................................................... 304
no spanning-tree max-age .................................................................... 304
no spanning-tree max-hops ................................................................... 304
no spanning-tree mode ......................................................................... 305
no spanning-tree mst ............................................................................. 306
no spanning-tree mst instance ............................................................... 306
no spanning-tree mst priority ............................................................... 307
no spanning-tree mst vlan ..................................................................... 307
no spanning-tree port mode ................................................................. 307
no spanning-tree port mode all ............................................................... 308
no spanning-tree tcnguard ..................................................................... 308
no spanning-tree uplinkfast ................................................................. 309
no split-horizon ................................................................................... 636
no sshcon maxsessions ......................................................................... 35
no sshcon timeout ................................................................................ 36
no stats flow-based .............................................................................. 265
no stats flow-based .............................................................................. 266
no stats group ..................................................................................... 264
no stats group ..................................................................................... 265
no storm-control broadcast ................................................................. 375
no storm-control broadcast action ......................................................... 375
no storm-control broadcast level .......................................................... 376
no storm-control broadcast rate ............................................................ 376
no storm-control multicast ................................................................. 377
no storm-control multicast action ......................................................... 377
no storm-control multicast level .......................................................... 378
no storm-control multicast rate ............................................................ 378
no storm-control unicast ................................................................. 379
no storm-control unicast action .................................................. 379
no storm-control unicast level ...................................................... 380
no storm-control unicast rate ....................................................... 380
no switchport access vlan ............................................................ 343
no switchport mode ................................................................. 341
no switchport mode private-vlan ................................................. 340
no switchport private-vlan ........................................................ 340
no switchport protected (Global Config) .................................... 349
no switchport protected (Interface Config) ................................. 349
no switchport trunk allowed vlan ................................................. 342
no switchport trunk native vlan .................................................. 343
no sync interval ........................................................................ 273
no system-mac ........................................................................... 411
no system-priority ...................................................................... 411
no tacacs-server host ................................................................ 105
no tacacs-server host link-local ................................................ 105
no tacacs-server key .................................................................. 106
no tacacs-server source-interface ............................................. 107
no tacacs-server timeout .......................................................... 107
no telnetcon maxsessions .......................................................... 32
no telnetcon timeout .................................................................. 32
no terminal length .................................................................... 139
no time-range ........................................................................... 792
no timers advertise ..................................................................... 565
no timers pacing flood .............................................................. 601
no timers pacing lsa-group ....................................................... 691
no timers throttle spf ............................................................... 691
no track interface ...................................................................... 567
no track ip route ......................................................................... 567
no traffic-shape ......................................................................... 738
no transport ............................................................................. 271
no transport input telnet ........................................................... 31
no transport output telnet ........................................................ 31
no trapflags ............................................................................... 603
no trapflags .............................................................................. 693
no username ............................................................................ 53
no username snmpv3 accessmode .............................................. 54
no username snmpv3 authentication ......................................... 55
no username snmpv3 encryption ............................................... 55
no vlan .................................................................................... 326
no vlan acceptframe ............................................................... 326
no vlan association mac ........................................................... 333
no vlan association subnet ........................................................ 333
no vlan ingressfilter ............................................................... 326
no vlan name ........................................................................... 327
no vlan port acceptframe all ..................................................... 329
no vlan port ingressfilter all ..................................................... 329
no vlan port pvid all ............................................................... 329
no vlan port tagging all ........................................................... 330
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer detection enable</td>
<td>408</td>
</tr>
<tr>
<td>peer detection interval</td>
<td>409</td>
</tr>
<tr>
<td>peer-keepalive destination</td>
<td>409</td>
</tr>
<tr>
<td>peer-keepalive enable</td>
<td>409</td>
</tr>
<tr>
<td>peer-keepalive timeout</td>
<td>410</td>
</tr>
<tr>
<td>Per-Command Authorization</td>
<td>49</td>
</tr>
<tr>
<td>periodic</td>
<td>793</td>
</tr>
<tr>
<td>permit ip host mac host</td>
<td>446</td>
</tr>
<tr>
<td>ping</td>
<td>156</td>
</tr>
<tr>
<td>ping ipv6</td>
<td>649</td>
</tr>
<tr>
<td>ping ipv6 interface</td>
<td>650</td>
</tr>
<tr>
<td>poe</td>
<td>281</td>
</tr>
<tr>
<td>poe detection</td>
<td>282</td>
</tr>
<tr>
<td>poe high-power</td>
<td>282</td>
</tr>
<tr>
<td>poe power limit</td>
<td>283</td>
</tr>
<tr>
<td>poe power management</td>
<td>283</td>
</tr>
<tr>
<td>poe priority</td>
<td>284</td>
</tr>
<tr>
<td>poe reset</td>
<td>284</td>
</tr>
<tr>
<td>poe timer schedule</td>
<td>284</td>
</tr>
<tr>
<td>poe traps</td>
<td>285</td>
</tr>
<tr>
<td>poe usagethreshold</td>
<td>285</td>
</tr>
<tr>
<td>police-simple</td>
<td>753</td>
</tr>
<tr>
<td>police-single-rate</td>
<td>754</td>
</tr>
<tr>
<td>police-two-rate</td>
<td>754</td>
</tr>
<tr>
<td>policy-map</td>
<td>754</td>
</tr>
<tr>
<td>policy-map rename</td>
<td>755</td>
</tr>
<tr>
<td>port</td>
<td>108</td>
</tr>
<tr>
<td>port</td>
<td>151</td>
</tr>
<tr>
<td>port</td>
<td>89</td>
</tr>
<tr>
<td>port lacpmode</td>
<td>398</td>
</tr>
<tr>
<td>port lacpmode enable all</td>
<td>398</td>
</tr>
<tr>
<td>port lacptimeout (Global Config)</td>
<td>399</td>
</tr>
<tr>
<td>port lacptimeout (Interface Config)</td>
<td>398</td>
</tr>
<tr>
<td>port-channel</td>
<td>390</td>
</tr>
<tr>
<td>port-channel adminmode</td>
<td>399</td>
</tr>
<tr>
<td>port-channel linktrap</td>
<td>400</td>
</tr>
<tr>
<td>port-channel load-balance</td>
<td>400</td>
</tr>
<tr>
<td>port-channel local-preference</td>
<td>401</td>
</tr>
<tr>
<td>port-channel min-links</td>
<td>401</td>
</tr>
<tr>
<td>port-channel name</td>
<td>401</td>
</tr>
<tr>
<td>port-channel static</td>
<td>397</td>
</tr>
<tr>
<td>port-channel system priority</td>
<td>402</td>
</tr>
<tr>
<td>port-security</td>
<td>470</td>
</tr>
<tr>
<td>port-security mac-address</td>
<td>471</td>
</tr>
<tr>
<td>port-security mac-address move</td>
<td>472</td>
</tr>
<tr>
<td>port-security mac-address sticky</td>
<td>472</td>
</tr>
<tr>
<td>port-security max-dynamic</td>
<td>471</td>
</tr>
<tr>
<td>port-security max-static</td>
<td>471</td>
</tr>
<tr>
<td>preempt</td>
<td>563</td>
</tr>
<tr>
<td>prefix-delegation (IPv6)</td>
<td>717</td>
</tr>
</tbody>
</table>
prefix-suppression (Router OSPF Config) ................................................................................................... 598
prefix-suppression (Router OSPFv3 Config) ................................................................................................... 598
priority ......................................................................................................................................................... 564
priority (TACACS Config) ............................................................................................................................ 108
priority1 ....................................................................................................................................................... 270
priority2 ....................................................................................................................................................... 270
private-vlan .................................................................................................................................................... 340
process cpu threshold .................................................................................................................................. 131
profile telecom g.8275.1 .................................................................................................................................. 269
protection-group (configure) .......................................................................................................................... 741
protection-group (interface) .................................................................................................................................. 756
protocol group ................................................................................................................................................ 331
protocol vlan group ....................................................................................................................................... 331
protocol vlan group all .................................................................................................................................. 331
ptp clock boundary domain ............................................................................................................................ 269
ptp enable ..................................................................................................................................................... 268
ptp udp debug .............................................................................................................................................. 273
quit ................................................................................................................................................................. 158
radius accounting mode .................................................................................................................................. 89
radius server attribute .................................................................................................................................... 90
radius server host .......................................................................................................................................... 91
radius server host link-local ............................................................................................................................ 92
radius server key .......................................................................................................................................... 93
radius server msgauth .................................................................................................................................... 93
radius server primary ..................................................................................................................................... 94
radius server retransmit .................................................................................................................................. 94
radius server timeout ..................................................................................................................................... 95
radius source-interface ................................................................................................................................... 95
random-detect .................................................................................................................................................. 736
random-detect exponential weighting-constant .............................................................................................. 737
random-detect queue-parms ............................................................................................................................ 737
redirect ............................................................................................................................................................ 751
redistribute (OSPF) ....................................................................................................................................... 599
redistribute (OSPFv3) ..................................................................................................................................... 690
redistribute (RIP) ............................................................................................................................................ 636
release dhcp ................................................................................................................................................... 517
reload ............................................................................................................................................................. 158
remark ............................................................................................................................................................ 766
remote-span ..................................................................................................................................................... 766
renew dhcp .................................................................................................................................................... 518
renew dhcp network-port .................................................................................................................................. 518
renew dhcp service-port .................................................................................................................................... 518
rmon alarm ..................................................................................................................................................... 518
rmon collection history ................................................................................................................................... 250
rmon event ....................................................................................................................................................... 250
rmon hcalarm .................................................................................................................................................. 251
role priority ..................................................................................................................................................... 410
route-map ........................................................................................................................................................ 538
show arp access-list ................................................................. 449
show arp brief ................................................................. 514
show arp switch .............................................................. 118
show arp switch .............................................................. 514
show authentication authentication-history ......................... 363
show authentication interface ............................................. 364
show authentication methods ............................................. 365
show authentication statistics .......................................... 365
show authorization methods ............................................. 51
show autoinstall .................................................................. 116
show auto-voip .................................................................... 797
show auto-voip oui-table .................................................. 798
show board address ........................................................... 163
show board cpu-load .......................................................... 164
show board memory-usage ................................................. 164
show board port-map .......................................................... 163
show board port-map all ..................................................... 163
show board port-map descr ................................................. 163
show board port-map list .................................................... 163
show board post-status ...................................................... 164
show board sensors ............................................................ 166
show board version ............................................................. 164
show bootpdhcprelay .......................................................... 576
show bootvar ...................................................................... 118
show bpdus forwarding ....................................................... 407
show capture packets .......................................................... 197
show chkconfig ................................................................. 169
show class-map ................................................................. 757
show classofservice dot1p-mapping ................................. 739
show classofservice ip-dscp-mapping ............................... 738
show classofservice ip-precedence-mapping .................... 739
show classofservice trust ................................................. 739
show clibanner ................................................................. 111
show clock ........................................................................ 177
show clock detail .............................................................. 177
show cpu-traffic ................................................................. 200
show cpu-traffic interface .................................................. 201
show cpu-traffic summary ................................................. 201
show cpu-traffic trace ........................................................ 202
show dampening interface .................................................. 610
show debugging ................................................................. 221
show dhcp client vendor-id-option .................................... 434
show dhcp l2relay agent-option vlan .................................. 432
show dhcp l2relay all .......................................................... 430
show dhcp l2relay circuit-id vlan ...................................... 431
show dhcp l2relay interface ................................................. 431
show dhcp l2relay remote-id vlan ..................................... 431
show dhcp l2relay stats interface ...................................... 431
show dhcp l2relay subscription interface ......................... 432
show dhcp l2relay vlan ........................................................ 433
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dhcp lease</td>
<td>522</td>
</tr>
<tr>
<td>show diffserv</td>
<td>758</td>
</tr>
<tr>
<td>show diffserv service</td>
<td>760</td>
</tr>
<tr>
<td>show diffserv service brief</td>
<td>761</td>
</tr>
<tr>
<td>show domain-name</td>
<td>71</td>
</tr>
<tr>
<td>show dos-control</td>
<td>496</td>
</tr>
<tr>
<td>show dot1q-tunnel</td>
<td>338</td>
</tr>
<tr>
<td>show dot1x</td>
<td>366</td>
</tr>
<tr>
<td>show dot1x authentication-history</td>
<td>370</td>
</tr>
<tr>
<td>show dot1x clients</td>
<td>370</td>
</tr>
<tr>
<td>show dot1x statistics</td>
<td>373</td>
</tr>
<tr>
<td>show dot1x users</td>
<td>371</td>
</tr>
<tr>
<td>show dvlan-tunnel</td>
<td>339</td>
</tr>
<tr>
<td>show errdisable recovery</td>
<td>506</td>
</tr>
<tr>
<td>show eventlog</td>
<td>119</td>
</tr>
<tr>
<td>show exception</td>
<td>227</td>
</tr>
<tr>
<td>show exception core-dump-file</td>
<td>227</td>
</tr>
<tr>
<td>show exception log</td>
<td>228</td>
</tr>
<tr>
<td>show fiber-ports optical-transceiver</td>
<td>128</td>
</tr>
<tr>
<td>show fiber-ports optical-transceiver-info</td>
<td>129</td>
</tr>
<tr>
<td>show flowcontrol</td>
<td>348</td>
</tr>
<tr>
<td>show forwardingdb agetime</td>
<td>498</td>
</tr>
<tr>
<td>show garp</td>
<td>351</td>
</tr>
<tr>
<td>show gmrp configuration</td>
<td>354</td>
</tr>
<tr>
<td>show gvrp configuration</td>
<td>352</td>
</tr>
<tr>
<td>show hardware</td>
<td>119</td>
</tr>
<tr>
<td>show hashdest</td>
<td>402</td>
</tr>
<tr>
<td>show hosts</td>
<td>193</td>
</tr>
<tr>
<td>show igmpsnooping</td>
<td>454</td>
</tr>
<tr>
<td>show igmpsnooping mrouter interface</td>
<td>455</td>
</tr>
<tr>
<td>show igmpsnooping mrouter vlan</td>
<td>456</td>
</tr>
<tr>
<td>show igmpsnooping querier</td>
<td>459</td>
</tr>
<tr>
<td>show igmpsnooping ssm</td>
<td>456</td>
</tr>
<tr>
<td>show interface</td>
<td>120</td>
</tr>
<tr>
<td>show interface counters</td>
<td>122</td>
</tr>
<tr>
<td>show interface dampening</td>
<td>610</td>
</tr>
<tr>
<td>show interface ethernet</td>
<td>123</td>
</tr>
<tr>
<td>show interface ethernet switchport</td>
<td>127</td>
</tr>
<tr>
<td>show interface lag</td>
<td>127</td>
</tr>
<tr>
<td>show interface loopback</td>
<td>652</td>
</tr>
<tr>
<td>show interface media-type</td>
<td>293</td>
</tr>
<tr>
<td>show interface tunnel</td>
<td>651</td>
</tr>
<tr>
<td>show interfaces cos-queue</td>
<td>739</td>
</tr>
<tr>
<td>show interfaces random-detect</td>
<td>740</td>
</tr>
<tr>
<td>show interfaces status</td>
<td>121</td>
</tr>
<tr>
<td>show interfaces status err-disabled</td>
<td>507</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>343</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>344</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>350</td>
</tr>
<tr>
<td>show interfaces tail-drop-threshold</td>
<td>740</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>show ipv6 brief</td>
<td>665</td>
</tr>
<tr>
<td>show ipv6 dhcp</td>
<td>718</td>
</tr>
<tr>
<td>show ipv6 dhcp binding</td>
<td>719</td>
</tr>
<tr>
<td>show ipv6 dhcp interface</td>
<td>668</td>
</tr>
<tr>
<td>show ipv6 dhcp interface</td>
<td>719</td>
</tr>
<tr>
<td>show ipv6 dhcp pool</td>
<td>720</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping</td>
<td>726</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping binding</td>
<td>727</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping database</td>
<td>728</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping interfaces</td>
<td>728</td>
</tr>
<tr>
<td>show ipv6 dhcp snooping statistics</td>
<td>728</td>
</tr>
<tr>
<td>show ipv6 dhcp statistics</td>
<td>718</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>666</td>
</tr>
<tr>
<td>show ipv6 interface vlan</td>
<td>668</td>
</tr>
<tr>
<td>show ipv6 mld groups</td>
<td>859</td>
</tr>
<tr>
<td>show ipv6 mld interface</td>
<td>861</td>
</tr>
<tr>
<td>show ipv6 mld traffic</td>
<td>862</td>
</tr>
<tr>
<td>show ipv6 mld-proxy</td>
<td>863</td>
</tr>
<tr>
<td>show ipv6 mld-proxy groups</td>
<td>865</td>
</tr>
<tr>
<td>show ipv6 mld-proxy groups detail</td>
<td>865</td>
</tr>
<tr>
<td>show ipv6 mld-proxy interface</td>
<td>864</td>
</tr>
<tr>
<td>show ipv6 mroute</td>
<td>843</td>
</tr>
<tr>
<td>show ipv6 mroute group</td>
<td>843</td>
</tr>
<tr>
<td>show ipv6 mroute source</td>
<td>844</td>
</tr>
<tr>
<td>show ipv6 mroute static</td>
<td>844</td>
</tr>
<tr>
<td>show ipv6 nd raguard policy</td>
<td>669</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>669</td>
</tr>
<tr>
<td>show ipv6 ospf</td>
<td>701</td>
</tr>
<tr>
<td>show ipv6 ospf abr</td>
<td>703</td>
</tr>
<tr>
<td>show ipv6 ospf area</td>
<td>704</td>
</tr>
<tr>
<td>show ipv6 ospf asbr</td>
<td>704</td>
</tr>
<tr>
<td>show ipv6 ospf database</td>
<td>705</td>
</tr>
<tr>
<td>show ipv6 ospf database database-summary</td>
<td>705</td>
</tr>
<tr>
<td>show ipv6 ospf interface</td>
<td>706</td>
</tr>
<tr>
<td>show ipv6 ospf interface brief</td>
<td>707</td>
</tr>
<tr>
<td>show ipv6 ospf interface stats</td>
<td>707</td>
</tr>
<tr>
<td>show ipv6 ospf lsa-group</td>
<td>708</td>
</tr>
<tr>
<td>show ipv6 ospf max-metric</td>
<td>709</td>
</tr>
<tr>
<td>show ipv6 ospf neighbor</td>
<td>710</td>
</tr>
<tr>
<td>show ipv6 ospf range</td>
<td>711</td>
</tr>
<tr>
<td>show ipv6 ospf statistics</td>
<td>711</td>
</tr>
<tr>
<td>show ipv6 ospf stub table</td>
<td>712</td>
</tr>
<tr>
<td>show ipv6 ospf virtual-link</td>
<td>713</td>
</tr>
<tr>
<td>show ipv6 ospf virtual-link brief</td>
<td>713</td>
</tr>
<tr>
<td>show ipv6 pim</td>
<td>852</td>
</tr>
<tr>
<td>show ipv6 pim bsr-router</td>
<td>855</td>
</tr>
<tr>
<td>show ipv6 pim interface</td>
<td>853</td>
</tr>
<tr>
<td>show ipv6 pim neighbor</td>
<td>854</td>
</tr>
<tr>
<td>show ipv6 pim rp mapping</td>
<td>856</td>
</tr>
<tr>
<td>show ipv6 pim rp-hash</td>
<td>855</td>
</tr>
</tbody>
</table>
show ipv6 pim ssm ............................................................................................................... 853
show ipv6 prefix-list ........................................................................................................ 547
show ipv6 protocols ....................................................................................................... 670
show ipv6 route .............................................................................................................. 670
show ipv6 route ecmp-groups .......................................................................................... 672
show ipv6 route hw-failure .............................................................................................. 672
show ipv6 route net-prototype ...................................................................................... 673
show ipv6 route preferences .......................................................................................... 673
show ipv6 route summary ............................................................................................... 674
show ipv6 snooping counters .......................................................................................... 675
show ipv6 source binding .............................................................................................. 731
show ipv6 traffic .............................................................................................................. 676
show ipv6 verify .............................................................................................................. 730
show ipv6 verify source .................................................................................................. 730
show ipv6 vlan ................................................................................................................ 676
show iscsi ........................................................................................................................ 801
show iscsi sessions ......................................................................................................... 802
show isdp ....................................................................................................................... 501
show isdp entry .............................................................................................................. 503
show isdp interface ......................................................................................................... 502
show isdp neighbors ....................................................................................................... 503
show isdp traffic ............................................................................................................. 504
show keepalive ............................................................................................................... 324
show keepalive statistics ............................................................................................... 324
show lacp actor .............................................................................................................. 404
show lacp partner .......................................................................................................... 404
show link state group ..................................................................................................... 383
show link state group detail ........................................................................................... 383
show lldp ......................................................................................................................... 477
show lldp interface ......................................................................................................... 477
show lldp local-device ..................................................................................................... 480
show lldp local-device detail ......................................................................................... 480
show lldp med ................................................................................................................ 483
show lldp med interface .................................................................................................. 484
show lldp med local-device detail ................................................................................ 485
show lldp med remote-device ....................................................................................... 486
show lldp med remote-device detail ............................................................................. 486
show lldp remote-device ............................................................................................... 478
show lldp remote-device detail ..................................................................................... 479
show lldp statistics ......................................................................................................... 478
show lpf interface .......................................................................................................... 384
show logging .................................................................................................................. 144
show logging backtrace ................................................................................................. 165
show logging buffered ................................................................................................... 145
show logging email config ............................................................................................ 150
show logging email statistics ....................................................................................... 150
show logging errcounter .............................................................................................. 165
show logging hosts ........................................................................................................ 146
show logging persistent ................................................................................................. 146
show logging traplogs ................................................................................................... 147
show loginsession ................................................................. 45
show loginsession long ..................................................... 46
show mac access-lists .......................................................... 767
show mac-address-table gmrp ............................................. 354
show mac-address-table igmp-snooping .................................. 456
show mac-address-table mld-snooping .................................. 467
show mac-address-table multicast ....................................... 498
show mac-address-table static ............................................ 426
show mac-address-table static-filtering ............................. 427
show mac-address-table stats ............................................. 499
show mac-addr-table .......................................................... 130
show mac-learn ................................................................. 298
show mail-server config .................................................... 152
show mbuf ................................................................. 228
show mbuf total ................................................................. 229
show mldsnooping ............................................................ 464
show mldsnooping mrouter interface .................................. 466
show mldsnooping mrouter vlan ......................................... 466
show mldsnooping querier .................................................. 469
show mldsnooping ssm entries ............................................. 466
show mldsnooping ssm groups ............................................ 467
show mldsnooping ssm stats ............................................... 467
show monitor session ........................................................ 422
show msg-queue ............................................................... 229
show mvr ................................................................. 387
show mvr interface ........................................................... 388
show mvr members ............................................................ 388
show mvr traffic ............................................................... 388
show network ................................................................. 25
show network ipv6 dhcp statistics ....................................... 720
show network ipv6 neighbors .............................................. 648
show packet-trace ecmp ...................................................... 230
show packet-trace lag ........................................................ 231
show packet-trace packet-data .......................................... 231
show packet-trace port ...................................................... 232
show packet-trace port eth .................................................. 233
show packet-trace port ipv4 .................................................. 233
show packet-trace port ipv6 .................................................. 234
show packet-trace port tcpv4 ............................................... 234
show packet-trace port tcpv6 ............................................... 234
show packet-trace port udpv4 ............................................... 235
show packet-trace port udpv6 ............................................... 235
show passwords configuration ........................................... 65
show passwords result ........................................................ 65
show platform ptp ............................................................. 278
show platform ptp state ...................................................... 277
show platform ptp stats ..................................................... 278
show platform ptp stats detailed .......................................... 279
show platform vpd ............................................................ 120
show poe ................................................................. 286
show tech-support ........................................................................................................... 138
show telnet .................................................................................................................... 33
show telnetcon ............................................................................................................. 33
show terminal length .................................................................................................. 139
show time-range .......................................................................................................... 794
show trapflags ............................................................................................................ 84
show users .................................................................................................................... 55
show users accounts ..................................................................................................... 56
show users login-history [long] ...................................................................................... 57
show users login-history [username] ............................................................................. 57
show users long ............................................................................................................ 56
show version ................................................................................................................ 119
show vlan .................................................................................................................... 333
show vlan association mac .......................................................................................... 336
show vlan association subnet ....................................................................................... 336
show vlan brief ............................................................................................................. 335
show vlan internal usage ............................................................................................. 334
show vlan port ............................................................................................................. 335
show vlan remote-span ............................................................................................... 424
show voice vlan .......................................................................................................... 346
show vpc ...................................................................................................................... 412
show vpc brief .............................................................................................................. 413
show vpc consistency-parameters ............................................................................... 414
show vpc peer-keepalive ............................................................................................. 415
show vpc role ............................................................................................................... 415
show vpc statistics ...................................................................................................... 416
show vrrp ..................................................................................................................... 568
show vrrp brief ............................................................................................................ 572
show vrrp statistics .................................................................................................... 572
show xxx|begin “string” ............................................................................................... 117
show xxx|exclude “string” ........................................................................................... 117
show xxx|include “string” ......................................................................................... 116
show xxx|include “string” exclude “string2” ................................................................. 117
show xxx|section “string” .......................................................................................... 117
show xxx|section “string” “string2” ............................................................................ 118
show xxx|section “string” include “string2” ................................................................. 118
shutdown ..................................................................................................................... 292
shutdown all ................................................................................................................. 292
snmp trap link-status .................................................................................................. 74
snmp trap link-status all ............................................................................................. 74
snmp-server ................................................................................................................ 71
snmp-server community .............................................................................................. 71
snmp-server community-group ................................................................................... 71
snmp-server enable traps ............................................................................................ 72
snmp-server enable traps all ........................................................................................ 73
snmp-server enable traps linkmode ............................................................................ 75
snmp-server enable traps multiusers .......................................................................... 75
snmp-server enable traps sfp ..................................................................................... 168
snmp-server enable traps stpmode ............................................................................. 75
snmp-server enable traps violation ................................................................. 72
snmp-server enable traps vrp ....................................................................... 562
snmp-server engineID local ........................................................................... 76
snmp-server filter ......................................................................................... 76
snmp-server group ......................................................................................... 77
snmp-server host ......................................................................................... 78
snmp-server port ......................................................................................... 73
snmp-server user ......................................................................................... 78
snmp-server v3-host ...................................................................................... 80
snmp-server view ......................................................................................... 79
snmptrap ip6addr snmpversion ....................................................................... 81
snmptrap ipaddr snmpversion ........................................................................ 81
snmptrap source-interface ............................................................................ 80
snntp broadcast client poll-interval ............................................................. 169
snntp client mode ....................................................................................... 170
snntp client port ......................................................................................... 170
snntp multicast client poll-interval ............................................................ 171
snntp server ............................................................................................... 172
snntp source-interface ............................................................................... 172
snntp unicast client poll-interval .............................................................. 170
snntp unicast client poll-retry ..................................................................... 171
snntp unicast client poll-timeout ............................................................... 171
spanning-tree .............................................................................................. 298
spanning-tree auto-edge ............................................................................... 298
spanning-tree backbonefast ........................................................................ 299
spanning-tree bpdufilter ............................................................................. 300
spanning-tree bpdufilter default ................................................................. 300
spanning-tree bpduflood ............................................................................. 300
spanning-tree bpduguard ............................................................................ 301
spanning-tree bpdumigrationcheck ............................................................. 301
spanning-tree configuration name ............................................................. 301
spanning-tree configuration revision .......................................................... 302
spanning-tree cost ...................................................................................... 302
spanning-tree edgeport .............................................................................. 302
spanning-tree forceversion ........................................................................ 303
spanning-tree forward-time ........................................................................ 303
spanning-tree guard ................................................................................. 303
spanning-tree max-age ............................................................................... 304
spanning-tree max-hops ............................................................................ 304
spanning-tree mode .................................................................................. 305
spanning-tree mst ...................................................................................... 305
spanning-tree mst instance ........................................................................ 306
spanning-tree mst priority ......................................................................... 306
spanning-tree mst vlan ............................................................................. 307
spanning-tree port mode ........................................................................... 307
spanning-tree port mode all ....................................................................... 307
spanning-tree port-priority ........................................................................ 308
spanning-tree tcnguard ............................................................................... 308
spanning-tree transmit .............................................................................. 308
spanning-tree uplinkfast ............................................................................ 309
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan routing</td>
<td>552</td>
</tr>
<tr>
<td>vlan tagging</td>
<td>332</td>
</tr>
<tr>
<td>voice vlan (Global Config)</td>
<td>345</td>
</tr>
<tr>
<td>voice vlan (Interface Config)</td>
<td>345</td>
</tr>
<tr>
<td>voice vlan data priority</td>
<td>345</td>
</tr>
<tr>
<td>vpc</td>
<td>411</td>
</tr>
<tr>
<td>vpc domain</td>
<td>408</td>
</tr>
<tr>
<td>vpc peer-link</td>
<td>412</td>
</tr>
<tr>
<td>vrrp</td>
<td>563</td>
</tr>
<tr>
<td>watchdog clear</td>
<td>236</td>
</tr>
<tr>
<td>watchdog disable</td>
<td>236</td>
</tr>
<tr>
<td>watchdog enable</td>
<td>236</td>
</tr>
<tr>
<td>write core</td>
<td>226</td>
</tr>
<tr>
<td>write memory</td>
<td>166</td>
</tr>
</tbody>
</table>
About Kontron

Kontron, a global leader in embedded computing technology and trusted advisor in IoT, works closely with its customers, allowing them to focus on their core competencies by offering a complete and integrated portfolio of hardware, software and services designed to help them make the most of their applications.

With a significant percentage of employees in research and development, Kontron creates many of the standards that drive the world’s embedded computing platforms; bringing to life numerous technologies and applications that touch millions of lives. The result is an accelerated time-to-market, reduced total-cost-of-ownership, product longevity and the best possible overall application with leading-edge, highest reliability embedded technology.

Kontron is a listed company. Its shares are traded in the Prime Standard segment of the Frankfurt Stock Exchange and on other exchanges under the symbol “KBC”. For more information, please visit: http://www.kontron.com/

CORPORATE OFFICES

EUROPE, MIDDLE EAST & AFRICA
Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com

NORTH AMERICA
14118 Stowe Drive
Poway, CA 92064-7147
USA
Tel.: + 1 888 294 4558
Fax: + 1 858 677 0898
info@us.kontron.com

ASIA PACIFIC
1-2F, 10 Building, No. 8 Liangshuihe 2nd Street
Economical & Technological Development Zone
Beijing 100070, P.R.China
Tel.: + 86 10 63751188
Fax: + 86 10 83682438
info@kontron.cn