ProSafe Managed Switch
Command Line Interface (CLI)
User Manual

9.0.2
GSM5212P
GSM7212F
GSM7212P
GSM7224P
XSM7224S
© 2011 NETGEAR, Inc. All rights reserved.
No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support
Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR
Phone (Other Countries): See Support information card.

Trademarks
NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions
To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

<table>
<thead>
<tr>
<th>Publication Part Number</th>
<th>Version</th>
<th>Publish Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-10936-01</td>
<td>1.0</td>
<td>November 2011</td>
<td>Add PoE and MVR mode features.</td>
</tr>
<tr>
<td>202-10515-05</td>
<td>1.1</td>
<td>June 2011</td>
<td>Add DHCPv6 and DHCPv6 mode features.</td>
</tr>
<tr>
<td>202-10515-04</td>
<td>1.0</td>
<td>November 2010</td>
<td>New document template.</td>
</tr>
<tr>
<td>202-10515-03</td>
<td>v 1.0</td>
<td>June 2010</td>
<td>Move some content to the Software Setup Guide.</td>
</tr>
<tr>
<td>202-10515-02</td>
<td></td>
<td></td>
<td>Software release 8.0.2: new firmware with DHCP L3 Relay, color conform policy, DHCP server in dynamic mode, and configuring a stacking port as an Ethernet port.</td>
</tr>
<tr>
<td>202-10515-01</td>
<td></td>
<td></td>
<td>Original publication.</td>
</tr>
</tbody>
</table>
## Contents

### Chapter 1 Using the Command-Line Interface

- Licensing and Command Support ........................................... 8
- Command Syntax ................................................................. 10
- Command Conventions .......................................................... 11
- Common Parameter Values ...................................................... 11
- Unit/Slot/Port Naming Convention ............................................ 12
- Using a Command’s “No” Form ................................................. 13
- Managed Switch Modules ...................................................... 13
- Command Modes ................................................................. 14
- Command Completion and Abbreviation .................................... 17
- CLI Error Messages ............................................................... 18
- CLI Line-Editing Conventions ............................................... 18
- Using CLI Help ................................................................. 19
- Accessing the CLI ............................................................... 20

### Chapter 2 Stacking Commands

- Dedicated Port Stacking ....................................................... 21
- Front Panel Stacking Commands ........................................... 29
- Non-Stop Forwarding Commands .......................................... 30
- Stack Firmware Synchronization Commands ......................... 34

### Chapter 3 Switching Commands

- Port Configuration Commands .............................................. 38
- Loopback Interface Commands .............................................. 44
- Spanning Tree Protocol (STP) Commands ............................... 46
- VLAN Commands .............................................................. 63
- Double VLAN Commands ................................................... 76
- Voice VLAN Commands ....................................................... 79
- Provisioning (IEEE 802.1p) Commands ................................ 81
- Protected Ports Commands .................................................. 81
- Private Group Commands .................................................... 84
- GARP Commands .............................................................. 85
- GVRP Commands ............................................................... 87
- GMRP Commands .............................................................. 89
- Port-Based Network Access Control Commands ..................... 91
- 802.1X Supplicant Commands ............................................. 105
- Storm-Control Commands ................................................... 107
- Port-Channel/LAG (802.3ad) Commands ................................. 118
- Port Mirroring ................................................................. 134
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static MAC Filtering</td>
<td>136</td>
</tr>
<tr>
<td>DHCP L2 Relay Agent Commands</td>
<td>140</td>
</tr>
<tr>
<td>DHCP Client Commands</td>
<td>144</td>
</tr>
<tr>
<td>DHCP Snooping Configuration Commands</td>
<td>145</td>
</tr>
<tr>
<td>Dynamic ARP Inspection Commands</td>
<td>154</td>
</tr>
<tr>
<td>IGMP Snooping Configuration Commands</td>
<td>161</td>
</tr>
<tr>
<td>IGMP Snooping Querier Commands</td>
<td>169</td>
</tr>
<tr>
<td>MLD Snooping Commands</td>
<td>172</td>
</tr>
<tr>
<td>MLD Snooping Querier Commands</td>
<td>179</td>
</tr>
<tr>
<td>set mld querier</td>
<td>179</td>
</tr>
<tr>
<td>set mld querier query_interval</td>
<td>180</td>
</tr>
<tr>
<td>set mld querier timer expiry</td>
<td>180</td>
</tr>
<tr>
<td>set mld querier election participate</td>
<td>181</td>
</tr>
<tr>
<td>show mldsnooping querier</td>
<td>181</td>
</tr>
<tr>
<td>Port Security Commands</td>
<td>182</td>
</tr>
<tr>
<td>LLDP (802.1AB) Commands</td>
<td>186</td>
</tr>
<tr>
<td>LLDP-MED Commands</td>
<td>194</td>
</tr>
<tr>
<td>Denial of Service Commands</td>
<td>203</td>
</tr>
<tr>
<td>MAC Database Commands</td>
<td>213</td>
</tr>
<tr>
<td>ISDP Commands</td>
<td>215</td>
</tr>
<tr>
<td>Priority-Based Flow Control Commands</td>
<td>220</td>
</tr>
<tr>
<td>Multicast VLAN Registration (MVR)</td>
<td>223</td>
</tr>
<tr>
<td>About MVR</td>
<td>223</td>
</tr>
<tr>
<td>MVR Commands</td>
<td>223</td>
</tr>
<tr>
<td>Routing Commands</td>
<td></td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP) Commands</td>
<td>232</td>
</tr>
<tr>
<td>IP Routing Commands</td>
<td>237</td>
</tr>
<tr>
<td>Router Discovery Protocol Commands</td>
<td>250</td>
</tr>
<tr>
<td>Virtual LAN Routing Commands</td>
<td>253</td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol Commands</td>
<td>254</td>
</tr>
<tr>
<td>DHCP and BOOTP Relay Commands</td>
<td>263</td>
</tr>
<tr>
<td>IP Helper Commands</td>
<td>265</td>
</tr>
<tr>
<td>Open Shortest Path First (OSPF) Commands</td>
<td>268</td>
</tr>
<tr>
<td>OSPF Graceful Restart Commands</td>
<td>305</td>
</tr>
<tr>
<td>nsf</td>
<td>306</td>
</tr>
<tr>
<td>nsf restart-interval</td>
<td>306</td>
</tr>
<tr>
<td>nsf helper</td>
<td>307</td>
</tr>
<tr>
<td>nsf helper disable</td>
<td>307</td>
</tr>
<tr>
<td>nsf [ietf] helper strict-lsa-checking</td>
<td>308</td>
</tr>
<tr>
<td>Routing Information Protocol (RIP) Commands</td>
<td>308</td>
</tr>
<tr>
<td>ICMP Throttling Commands</td>
<td>316</td>
</tr>
<tr>
<td>IP Multicast Commands</td>
<td>318</td>
</tr>
</tbody>
</table>
Chapter 7 IPv6 Commands

- Tunnel Interface Commands ........................................... 354
- IPv6 Routing Commands .................................................. 355
- OSPFv3 Commands .......................................................... 376
- OSPFv3 Graceful Restart Commands ................................. 407
- DHCPv6 Commands ......................................................... 409

Chapter 8 IPv6 Multicast Commands

- IPv6 Multicast Forwarder Commands ............................... 418
- IPv6 PIM Commands ....................................................... 420
- IPv6 MLD Commands ....................................................... 428
- IPv6 MLD-Proxy Commands ............................................. 434

Chapter 9 Quality of Service (QoS) Commands

- Class of Service (CoS) Commands .................................... 440
- Differentiated Services (DiffServ) Commands ...................... 448
- DiffServ Class Commands ............................................... 449
- DiffServ Policy Commands .............................................. 457
- DiffServ Service Commands ............................................ 463
- DiffServ Show Commands .............................................. 464
- MAC Access Control List (ACL) Commands ....................... 470
- IP Access Control List (ACL) Commands ......................... 474
- IPv6 Access Control List (ACL) Commands ....................... 481
- Time Range Commands for Time-Based ACLs .................... 485
- Auto-Voice over IP Commands ........................................ 488

Chapter 10 Power over Ethernet (PoE) Commands

- About PoE .................................................................... 490
- PoE Commands ............................................................. 491

Chapter 11 Utility Commands

- Auto Install Commands .................................................. 502
- Dual Image Commands .................................................... 504
- System Information and Statistics Commands .................... 506
- Logging Commands ......................................................... 516
- Email Alerting and Mail Server Commands ....................... 520
- System Utility and Clear Commands ................................. 527
- Simple Network Time Protocol (SNTP) Commands .............. 536
- DHCP Server Commands ............................................... 543
- DNS Client Commands ................................................... 555
<table>
<thead>
<tr>
<th>Command Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Capture Commands</td>
<td>560</td>
</tr>
<tr>
<td>Serviceability Packet Tracing Commands</td>
<td>561</td>
</tr>
<tr>
<td>Cable Test Command</td>
<td>579</td>
</tr>
<tr>
<td>sFlow Commands</td>
<td>579</td>
</tr>
<tr>
<td>Software License Commands</td>
<td>584</td>
</tr>
<tr>
<td>IP Address Conflict Commands</td>
<td>585</td>
</tr>
<tr>
<td>Link Local Protocol Filtering Commands</td>
<td>586</td>
</tr>
<tr>
<td>Cable Test Command</td>
<td>579</td>
</tr>
<tr>
<td>IP Address Conflict Commands</td>
<td>585</td>
</tr>
<tr>
<td>Link Local Protocol Filtering Commands</td>
<td>586</td>
</tr>
<tr>
<td>Software License Commands</td>
<td>584</td>
</tr>
<tr>
<td>IP Address Conflict Commands</td>
<td>585</td>
</tr>
<tr>
<td>Link Local Protocol Filtering Commands</td>
<td>586</td>
</tr>
<tr>
<td>Configuration Scripting Commands</td>
<td>655</td>
</tr>
<tr>
<td>Pre-login Banner and System Prompt Commands</td>
<td>657</td>
</tr>
<tr>
<td>Switch Database Management (SDM) Templates</td>
<td>658</td>
</tr>
<tr>
<td>IPv6 Management Commands</td>
<td>659</td>
</tr>
</tbody>
</table>

**Chapter 12 Management Commands**

- Configuring the Switch Management CPU: 589
- Network Interface Commands: 591
- Console Port Access Commands: 594
- Telnet Commands: 596
- Secure Shell (SSH) Commands: 601
- Management Security Commands: 604
- Hypertext Transfer Protocol (HTTP) Commands: 605
- Access Commands: 612
- User Account Commands: 612
- SNMP Commands: 628
- RADIUS Commands: 639
- TACACS+ Commands: 651
- Configuration Scripting Commands: 655
- Pre-login Banner and System Prompt Commands: 657
- Switch Database Management (SDM) Templates: 658
- IPv6 Management Commands: 659

**Chapter 13 Log Messages**

- Core: 665
- Utilities: 667
- Management: 669
- Switching: 673
- QoS: 679
- Routing/IPv6 Routing: 680
- Multicast: 683
- Stacking: 685
- Technologies: 686
- O/S Support: 688

**Chapter 14 Captive Portal Commands**

- Captive Portal Global Commands: 690
- Captive Portal Configuration Commands: 694
- Captive Portal Status Commands: 700
- Captive Portal Client Connection Commands: 704
- Captive Portal Interface Commands: 708
- Captive Portal Local User Commands: 709
- Captive Portal User Group Commands: 715
Chapter 15  Command List

Index
Using the Command-Line Interface

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

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

- Licensing and Command Support
- Command Syntax
- Command Conventions
- Common Parameter Values
- Unit/Slot/Port Naming Convention
- Using a Command’s “No” Form
- Managed Switch Modules
- Command Modes
- Command Completion and Abbreviation
- CLI Error Messages
- CLI Line-Editing Conventions
- Using CLI Help
- Accessing the CLI

**Licensing and Command Support**

As shown in the following table, some command groups or commands require a license and some are supported on particular switch models. For those requiring a license, license keys
are available from your VAR or NETGEAR authorized e-commerce portal. License activation is described in the Software Setup Manual.

<table>
<thead>
<tr>
<th>Command Group or Command</th>
<th>XSM7224S</th>
<th>GSM7212F/GSM7212P/GSM7224P/GSM5212P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front Panel Stacking Commands</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Non-Stop Forwarding Commands</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Stack Firmware Synchronization Commands</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Router Discovery Protocol Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>Open Shortest Path First (OSPF) Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>OSPF Graceful Restart Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>Routing Information Protocol (RIP) Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>Tunnel Interface Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>IPv6 Routing Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>OSPFv3 Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>OSPFv3 Graceful Restart Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>DHCPv6 Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>Multicast Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>DVMRP Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>PIM Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>Internet Group Message Protocol (IGMP) Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>IGMP Proxy Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>IPv6 Multicast Forwarder Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>IPv6 PIM Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>IPv6 MLD Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>IPv6 MLD-Proxy Commands</td>
<td>Require license</td>
<td>Not supported</td>
</tr>
<tr>
<td>PoE Commands</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>MVR Commands</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Link Local Protocol Filtering Commands</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Priority-Based Flow Control Commands</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Captive Portal Commands</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
ProSafe Managed Switch

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 New Template User Manual 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.
Command Conventions

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

The parameters for a command might include mandatory values, optional values, or keyword choices. **Table 1** describes the conventions this document uses to distinguish between value types.

**Table 1. Parameter Conventions**

<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>{[]} Braces within square brackets</td>
<td>[[choice1</td>
<td>choice2]]</td>
</tr>
</tbody>
</table>

Common Parameter Values

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System
Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. Table 2 describes common parameter values and value formatting.

**Table 2. Parameter Descriptions**

<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></td>
<td>For additional information, refer to RFC 3513.</td>
</tr>
<tr>
<td>Interface or</td>
<td>Valid slot and port number separated by forward slashes. For example, 0/1 represents slot number 0 and port number 1.</td>
</tr>
<tr>
<td>unit/slot/port</td>
<td>Logical Interface</td>
</tr>
<tr>
<td></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 unit/slot/port to configure the port-channel.</td>
</tr>
<tr>
<td>Character</td>
<td>Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.</td>
</tr>
<tr>
<td>strings</td>
<td></td>
</tr>
</tbody>
</table>

**Unit/Slot/Port Naming Convention**

Managed switch software references physical entities such as cards and ports by using a unit/slot/port naming convention. The 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. VLAN routing interfaces are only used for routing functions. Loopback interfaces are logical interfaces that are always up. Tunnel interfaces are logical point-to-point links that carry encapsulated packets.</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>

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

**Using a Command’s “No” Form**

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.

**Managed Switch Modules**

Managed switch 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 software.

The software suite includes the following modules:

- Switching (Layer 2)
- Routing (Layer 3)
- IPv6—IPv6 routing
- Multicast
• Quality of Service
• Management (CLI, Web UI, and SNMP)
• IPv6 Management—Allows management of the device through an IPv6 through an IPv6 address without requiring the IPv6 Routing package in the system. The management address can be associated with the network port (front-panel switch ports) and a routine interface (port or VLAN).
• Stacking

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

## Command Modes

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

The command prompt changes in each command mode to help you identify the current mode. Table 5 describes the command modes and the prompts visible in that mode.

---

**Note:** The command modes available on your switch depend on the software modules that are installed. For example, a switch that does not support BGPv4 does not have the Router BGPv4 Command Mode.

---

### Table 5. CLI Command Modes

<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>
</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>Interface Config</td>
<td>Switch (Interface &lt;unit/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>
<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>Ipv6_Class-Map Config</td>
<td>Switch (Config-class-map)#</td>
<td>Contains the QoS class map configuration commands for IPv6.</td>
</tr>
<tr>
<td>Router OSPF Config</td>
<td>Switch (Config-router)#</td>
<td>Contains the OSPF configuration commands.</td>
</tr>
<tr>
<td>Router OSPFv3 Config</td>
<td>Switch (Config rtr)#</td>
<td>Contains the OSPFv3 configuration commands.</td>
</tr>
<tr>
<td>Router RIP Config</td>
<td>Switch (Config-router)#</td>
<td>Contains the RIP configuration commands.</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>
<tr>
<td>DHCPv6 Pool Config</td>
<td>Switch (Config dhcp6-pool)#</td>
<td>Contains the DHCPv6 server IPv6 address pool configuration commands.</td>
</tr>
<tr>
<td>Stack Global Config Mode</td>
<td>Switch (Config stack)#</td>
<td>Allows you to access the Stack Global Config Mode.</td>
</tr>
<tr>
<td>ARP Access-List Config Mode</td>
<td>Switch (Config-arp-access-list)#</td>
<td>Contains commands to add ARP ACL rules in an ARP Access List.</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 <code>logout</code>.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>From the User EXEC mode, enter <code>enable</code>.</td>
<td>To exit to the User EXEC mode, enter <code>exit</code> or press <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Global Config</td>
<td>From the Privileged EXEC mode, enter <code>configure</code>.</td>
<td>To exit to the Privileged EXEC mode, enter <code>exit</code>, or press <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>VLAN Config</td>
<td>From the Privileged EXEC mode, enter <code>vlan database</code>.</td>
<td>To exit to the Privileged EXEC mode, enter <code>exit</code>, or press <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Interface Config</td>
<td>From the Global Config mode, enter <code>interface &lt;unit/slot/port&gt;</code> or <code>interface loopback &lt;id&gt;</code> or <code>interface tunnel &lt;id&gt;</code></td>
<td>To exit to the Global Config mode, enter <code>exit</code>. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Line Config</td>
<td>From the Global Config mode, enter <code>lineconfig</code>.</td>
<td>To exit to the Global Config mode, enter <code>exit</code>. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Policy-Map Config</td>
<td>From the Global Config mode, enter <code>policy-map &lt;name&gt; in.</code></td>
<td>To exit to the Global Config mode, enter <code>exit</code>. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Policy-Class-Map Config</td>
<td>From the Policy Map mode enter <code>class</code>.</td>
<td>To exit to the Policy Map mode, enter <code>exit</code>. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Class-Map Config</td>
<td>From the Global Config mode, enter <code>class-map</code>, and specify the optional keyword <code>ipv4</code> to specify the Layer 3 protocol for this class. See <code>class-map</code> on page 449 for more information.</td>
<td>To exit to the Global Config mode, enter <code>exit</code>. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Ipv6-Class-Map Config</td>
<td>From the Global Config mode, enter <code>class-map</code> and specify the optional keyword <code>ipv6</code> to specify the Layer 3 protocol for this class. See <code>class-map</code> on page 449 for more information.</td>
<td>To exit to the Global Config mode, enter <code>exit</code>. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Router OSPF Config</td>
<td>From the Global Config mode, enter <code>router ospf</code>.</td>
<td>To exit to the Global Config mode, enter <code>exit</code>. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code>.</td>
</tr>
<tr>
<td>Router OSPFv3 Config</td>
<td>From the Global Config mode, enter <code>ipv6 router ospf</code>.</td>
<td>To exit to the Global Config mode, enter <code>exit</code>. To return to the Privileged EXEC mode, enter <code>Ctrl-Z</code>.</td>
</tr>
</tbody>
</table>
Table 6. CLI Mode Access and Exit (Continued)

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Exit or Access Previous Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router RIP Config</td>
<td>From the Global Config mode, enter</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></td>
<td><code>router rip</code></td>
<td></td>
</tr>
<tr>
<td>MAC Access-list Config</td>
<td>From the Global Config mode, enter</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></td>
<td><code>mac access-list extended &lt;name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>TACACS Config</td>
<td>From the Global Config mode, enter</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></td>
<td><code>tacacs-server host &lt;ip-addr&gt;</code>, where &lt;ip-addr&gt; is the IP address of the TACACS server on your network.</td>
<td></td>
</tr>
<tr>
<td>DHCP Pool Config</td>
<td>From the Global Config mode, enter</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></td>
<td><code>ip dhcp pool &lt;pool-name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>DHCPv6 Pool Config</td>
<td>From the Global Config mode, enter</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></td>
<td><code>ip dhcpv6 pool &lt;pool-name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Stack Global Config Mode</td>
<td>From the Global Config mode, enter</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></td>
<td><code>stack</code> command</td>
<td></td>
</tr>
<tr>
<td>ARP Access-List Config Mode</td>
<td>From the Global Config mode, enter</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></td>
<td><code>arp access-list command</code></td>
<td></td>
</tr>
</tbody>
</table>

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.
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>

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>
</tbody>
</table>
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

**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 591.
This chapter contains the following sections:

- **Dedicated Port Stacking**
- **Front Panel Stacking Commands**
- **Non-Stop Forwarding Commands**
- **Stack Firmware Synchronization Commands**

The commands in this chapter are in 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.

The Primary Management Unit is the unit that controls the stack.

### Dedicated Port Stacking

This section describes the commands you use to configure dedicated port stacking.

**stack**

This command sets the mode to Stack Global Config.

**Format**

```
stack
```

**Mode**

Global Config

**member**

This command configures a switch. The `<unit>` is the switch identifier of the switch to be added/removed from the stack. The `<switchindex>` is the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer. This command is executed on the Primary Management Unit.

**Format**

```
member <unit> <switchindex>
```

**Mode**

Stack Global Config
Note: Switch index can be obtained by executing the show supported switchtype command in User EXEC mode.

no member

This command removes a switch from the stack. The `<unit>` is the switch identifier of the switch to be removed from the stack. This command is executed on the Primary Management Unit.

Format  no member <unit>
Mode    Stack Global Config

switch priority

This command configures the ability of a switch to become the Primary Management Unit. The `<unit>` is the switch identifier. The `<value>` is the preference parameter that allows the user to specify, priority of one backup switch over another. The range for priority is 1 to 15. The switch with the highest priority value will be chosen to become the Primary Management Unit if the active Primary Management Unit fails. The switch priority defaults to the hardware management preference value 1. Switches that do not have the hardware capability to become the Primary Management Unit are not eligible for management.

Default  enabled
Format    switch <unit> priority <value>
Mode      Global Config

switch renumber

This command changes the switch identifier for a switch in the stack. The `<oldunit>` is the current switch identifier on the switch whose identifier is to be changed. The `<newunit>` is the updated value of the switch identifier. Upon execution, the switch will be configured with the configuration information for the new switch, if any. The old switch configuration information will be retained, however the old switch will be operationally unplugged. This command is executed on the Primary Management Unit.

Note: If the management unit is renumbered, then the running configuration is no longer applied (i.e. the stack acts as if the configuration had been cleared)
movemanagement

This command moves the Primary Management Unit functionality from one switch to another. The `<fromunit>` is the switch identifier on the current Primary Management Unit. The `<tounit>` is the switch identifier on the new Primary Management Unit. Upon execution, the entire stack (including all interfaces in the stack) is unconfigured and reconfigured with the configuration on the new Primary Management Unit. After the reload is complete, all stack management capability must be performed on the new Primary Management Unit. To preserve the current configuration across a stack move, execute the `copy system:running-config nvram:startup-config` (in Privileged EXEC) command before performing the stack move. A stack move causes all routes and layer 2 addresses to be lost. This command is executed on the Primary Management Unit. The system prompts you to confirm the management move.

**Note:** The movemanagement command does not NSF (non-stop forwarding). To move the management unit to the backup unit, use `initiate failover` instead. For more information, see `initiate failover` on page 32.

```plaintext
Format: movemanagement <fromunit> <tounit>
Mode: Stack Global Config
```

standby

Use this command to configure a unit as a Standby Management Unit (STBY).

```plaintext
Format: standby <unit number>
Mode: Stack Global Config
```

**Note:** The Standby Management Unit cannot be the current Management Unit. The Standby unit should be a management-capable unit.

slot

This command configures a slot in the system. The `<unit/slot>` is the slot identifier of the slot. The `<cardindex>` is the index into the database of the supported card types.
indicating the type of the card being preconfigured in the specified slot. The card index is a 32-bit integer. If a card is currently present in the slot that is unconfigured, the configured information will be deleted and the slot will be re-configured with default information for the card.

**Format**
```
slot <unit/slot> <cardindex>
```

**Mode**
Global Config

**Note:** Card index can be obtained by executing show supported cardtype command in User EXEC mode.

---

**no slot**

This command removes configured information from an existing slot in the system.

**Format**
```
no slot <unit/slot> <cardindex>
```

**Mode**
Global Config

**Note:** Card index can be obtained by executing show supported cardtype command in User EXEC mode.

---

**set slot disable**

This command configures the administrative mode of the slot(s). If you specify [all], the command is applied to all slots, otherwise the command is applied to the slot identified by `<unit/slot>`.

If a card or other module is present in the slot, this administrative mode will effectively be applied to the contents of the slot. If the slot is empty, this administrative mode will be applied to any module that is inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as “unplugged” on management screens.

**Format**
```
set slot disable [<unit/slot> | all]
```

**Mode**
Global Config

---

**no set slot disable**

This command unconfigures the administrative mode of the slot(s). If you specify [all], the command removes the configuration from all slots, otherwise the configuration is removed from the slot identified by `<unit/slot>`.

If a card or other module is present in the slot, this administrative mode removes the configuration from the contents of the slot. If the slot is empty, this administrative mode
removes the configuration from any module inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as “unplugged” on management screens.

Format  no set slot disable [<unit/slot> | all]
Mode  Global Config

**set slot power**

This command configures the power mode of the slot(s) and allows power to be supplied to a card located in the slot. If you specify [all], the command is applied to all slots, otherwise the command is applied to the slot identified by <unit/slot>.

Use this command when installing or removing cards. If a card or other module is present in this slot, the power mode is applied to the contents of the slot. If the slot is empty, the power mode is applied to any card inserted into the slot.

Format  set slot power [<unit/slot> | all]
Mode  Global Config

**no set slot power**

This command unconfigures the power mode of the slot(s) and prohibits power from being supplied to a card located in the slot. If you specify [all], the command prohibits power to all slots, otherwise the command prohibits power to the slot identified by <unit/slot>.

Use this command when installing or removing cards. If a card or other module is present in this slot, power is prohibited to the contents of the slot. If the slot is empty, power is prohibited to any card inserted into the slot.

Format  no set slot power [<unit/slot> | all]
Mode  Global Config

**reload (Stack)**

This command resets the entire stack or the identified <unit>. The <unit> is the switch identifier. The system prompts you to confirm that you want to reset the switch.

Format  reload [<unit>]
Mode  User EXEC

**show slot**

This command displays information about all the slots in the system or for a specific slot.

Format  show slot [<unit/slot>]
Mode  User EXEC
Term | Definition
--- | ---
Slot | The slot identifier in a `<unit/slot>` format.
Slot Status | The slot is empty, full, or has encountered an error.
Admin State | The slot administrative mode is enabled or disabled.
Power State | The slot power mode is enabled or disabled.
Configured Card | The model identifier of the card preconfigured in the slot. Model Identifier is a 32-character field used to identify a card.
Model Identifier | Cards are pluggable or non-pluggable in the slot.
Pluggable | Indicates whether the slot can be powered down.
Power Down | The model identifier of the card inserted in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full.
Inserted Card Description | The card description. This field is displayed only if the slot is full.
Configured Card Description | The card description of the card preconfigured in the slot.

If you supply a value for `<unit/slot>`, the following additional information appears:

Term | Definition
--- | ---
Inserted Card Model Identifier | The model identifier of the card inserted in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full.
Inserted Card Description | The card description. This field is displayed only if the slot is full.
Configured Card Description | The card description of the card preconfigured in the slot.

### show supported cardtype

This command displays information about all card types or specific card types supported in the system.

**Format**

```
show supported cardtype [<cardindex>]
```

**Mode**

User EXEC

If you do not supply a value for `<cardindex>`, the following output appears:

Term | Definition
--- | ---
Card Index (CID) | The index into the database of the supported card types. This index is used when preconfiguring a slot.
Card Model Identifier | The model identifier for the supported card type.

If you supply a value for `<cardindex>`, the following output appears:

Term | Definition
--- | ---
Card Type | The 32-bit numeric card type for the supported card.
show switch

This command displays information about all units in the stack or a single unit when you specify the unit value.

Format  

```
show switch [<unit>]
```

Mode  Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Identifier</td>
<td>The model identifier for the supported card type.</td>
</tr>
<tr>
<td>Card Description</td>
<td>The description for the supported card type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>The unit identifier assigned to the switch.</td>
</tr>
</tbody>
</table>

When you do not specify a value for `<unit>`, the following information appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Status</td>
<td>Indicates whether the switch is the Primary Management Unit, a stack member, or the status is unassigned.</td>
</tr>
<tr>
<td>Preconfigured Model Identifier</td>
<td>The model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.</td>
</tr>
<tr>
<td>Plugged-In Model Identifier</td>
<td>The model identifier of the switch in the stack. Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.</td>
</tr>
<tr>
<td>Switch Status</td>
<td>The switch status. Possible values for this state are: OK, Unsup ported, Code Mismatch, Config Mismatch, or Not Present.</td>
</tr>
<tr>
<td>Code Version</td>
<td>The detected version of code on this switch.</td>
</tr>
</tbody>
</table>

When you specify a value for `<unit>`, the following information appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Status</td>
<td>Indicates whether the switch is the Primary Management Unit, a stack member, or the status is unassigned.</td>
</tr>
<tr>
<td>Hardware Management Preference</td>
<td>The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.</td>
</tr>
<tr>
<td>Admin Management Preference</td>
<td>The administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the Primary Management Unit.</td>
</tr>
<tr>
<td>Switch Type</td>
<td>The 32-bit numeric switch type.</td>
</tr>
</tbody>
</table>
ProSafe Managed Switch

### show supported switchtype

This command displays information about all supported switch types or a specific switch type.

**Format**

```
show supported switchtype [<switchindex>]
```

**Mode**

- User EXEC
- Privileged EXEC

If you do not supply a value for `<switchindex>`, the following output appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Index (SID)</td>
<td>The index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.</td>
</tr>
<tr>
<td>Model Identifier</td>
<td>The model identifier for the supported switch type.</td>
</tr>
<tr>
<td>Management Preference</td>
<td>The management preference value of the switch type.</td>
</tr>
<tr>
<td>Code Version</td>
<td>The code load target identifier of the switch type.</td>
</tr>
</tbody>
</table>

If you supply a value for `<switchindex>`, the following output appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Type</td>
<td>The 32-bit numeric switch type for the supported switch.</td>
</tr>
<tr>
<td>Model Identifier</td>
<td>The model identifier for the supported switch type.</td>
</tr>
<tr>
<td>Switch Description</td>
<td>The description for the supported switch type.</td>
</tr>
</tbody>
</table>
Front Panel Stacking Commands

This section describes the commands you use to view and configure front panel stacking information.

**stack-port**

This command sets front panel stacking per port to either stack or ethernet mode.

**Term** | **Definition**
--- | ---
Default | stack
Format | `stack-port <unit/slot/port> [{ethernet | stack}]`
Mode | Stack Global Config

**show stack-port**

This command displays summary stack-port information for all interfaces.

**Format** | **show stack-port**
--- | ---
**Mode** | Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>The unit number</td>
</tr>
<tr>
<td>Interface</td>
<td>The slot and port numbers.</td>
</tr>
<tr>
<td>Configured Stack Mode</td>
<td>Stack or Ethernet.</td>
</tr>
<tr>
<td>Running Stack Mode</td>
<td>Stack or Ethernet.</td>
</tr>
<tr>
<td>Link Status</td>
<td>Status of the link</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Speed (Gbps) of the stack port link.</td>
</tr>
</tbody>
</table>

**show stack-port counters**

This command displays summary data counter information for all interfaces.

**Format** | **show stack-port counters**
--- | ---
**Mode** | Privileged EXEC
show stack-port diag

This command shows front panel stacking diagnostics for each port and is only intended for Field Application Engineers (FAEs) and developers. An FAE will advise on the necessity to run this command and capture this information.

Format
show stack-port diag
Mode
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>The unit number.</td>
</tr>
<tr>
<td>Interface</td>
<td>The slot and port numbers.</td>
</tr>
<tr>
<td>Tx Data Rate</td>
<td>Trashing data rate in megabits per second on the stacking port.</td>
</tr>
<tr>
<td>Tx Error Rate</td>
<td>Platform-specific number of transmit errors per second.</td>
</tr>
<tr>
<td>Tx Total Error</td>
<td>Platform-specific number of total transmit errors since power-up.</td>
</tr>
<tr>
<td>Rx Data Rate</td>
<td>Receive data rate in megabits per second on the stacking port.</td>
</tr>
<tr>
<td>Rx Error Rate</td>
<td>Platform-specific number of receive errors per second.</td>
</tr>
<tr>
<td>Rx Total Errors</td>
<td>Platform-specific number of total receive errors since power-up.</td>
</tr>
</tbody>
</table>

Non-Stop Forwarding Commands

Non-stop forwarding allows the stack units to continue to forward packets if the stack management unit restarts because of a power failure, hardware failure, or software fault.

nsf

Use this command to enable nonstop forwarding feature on the stack. When nonstop forwarding is enabled, if the management unit of a stack fails, the backup unit takes over as the master without cleaning the hardware tables of any of the surviving units. Data traffic...
continues to be forwarded in hardware while the management functions initialize on the backup unit. NSF is enabled by default on platforms that support it. The administrator can disable NSF to redirect the CPU resources consumed by data checkpointing. If a unit that does not support NSF is connected to the stack, then NSF is disabled on all stack members. If a unit that does not support NSF is disconnected from the stack and all other units support NSF, and NSF is administratively enabled, then NSF operation resumes.

**Default**

<table>
<thead>
<tr>
<th>Format</th>
<th>nsf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Stack Global Config</td>
</tr>
</tbody>
</table>

**no nsf**

This command disables non-stop forwarding on the stack.

<table>
<thead>
<tr>
<th>Format</th>
<th>no nsf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Stack Global Config</td>
</tr>
</tbody>
</table>

**show nsf**

This command displays global and per-unit information on NSF configuration on the stack.

<table>
<thead>
<tr>
<th>Format</th>
<th>show nsf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSF Administrative Status</td>
<td>Whether nonstop forwarding is administratively enabled or disabled. Default: Enabled</td>
</tr>
<tr>
<td>NSF Operational Status</td>
<td>Indicates whether NSF is enabled on the stack.</td>
</tr>
<tr>
<td>Last Startup Reason</td>
<td>The type of activation that caused the software to start the last time:</td>
</tr>
<tr>
<td></td>
<td>• “Power-On” means that the switch rebooted. This could have been caused by a power cycle or an administrative “Reload” command.</td>
</tr>
<tr>
<td></td>
<td>• “Administrative Move” means that the administrator issued the movemanagement command for the stand-by manager to take over.</td>
</tr>
<tr>
<td></td>
<td>• “Warm-Auto-Restart” means that the primary management card restarted due to a failure, and the system executed a nonstop forwarding failover.</td>
</tr>
<tr>
<td></td>
<td>• “Cold-Auto-Restart” means that the system switched from the active manager to the backup manager and was unable to maintain user data traffic. This is usually caused by multiple failures occurring close together.</td>
</tr>
<tr>
<td>Time Since Last Restart Time</td>
<td>The time since the current management unit became the active management unit.</td>
</tr>
<tr>
<td>Restart in progress</td>
<td>Whether a restart is in progress.</td>
</tr>
</tbody>
</table>
### Example:

(Switch)#show nsf
Administrative Status.......................... Enable
Operational Status.............................. Enable
Last Startup Reason............................ Warm Auto-Restart
Time Since Last Restart........................ 0 days 16 hrs 52 mins 55 secs
Restart In Progress............................. No
Warm Restart Ready............................. Yes
Copy of Running Configuration to Backup Unit:
  Status........................................ Stale
  Time Since Last Copy........................ 0 days 4 hrs 53 mins 22 secs
  Time Until Next Copy........................ 28 seconds
Unit NSF Support
  1 Yes
  2 Yes
  3 Yes

### initiate failover

Use this command to force the backup unit to take over as the management unit and perform a “warm restart” of the stack. On a warm restart, the backup unit becomes the management unit without clearing its hardware tables (on a cold restart, hardware tables are cleared). Applications apply checkpointed data from the former management unit. The original management unit reboots. If the system is not ready for a warm restart, for example because no backup unit has been elected or one or more members of the stack do not support nonstop forwarding, the command fails with a warning message. The movemanagement command also transfers control from the current management unit; however, the hardware is cleared and all units reinitialize.

**Note:** Use this command instead of movemanagement if you expect nsf during management unit changes.
show checkpoint statistics

Use this command to display general information about the checkpoint service operation.

Format: show checkpoint statistics
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages Checkpointed</td>
<td>Number of checkpoint messages transmitted to the backup unit.</td>
</tr>
<tr>
<td></td>
<td>Range: Integer. Default: 0</td>
</tr>
<tr>
<td>Bytes Checkpointed</td>
<td>Number of bytes transmitted to the backup unit.</td>
</tr>
<tr>
<td></td>
<td>Range: Integer. Default: 0</td>
</tr>
<tr>
<td>Time Since Counters Cleared</td>
<td>Number of days, hours, minutes and seconds since the counters were reset to</td>
</tr>
<tr>
<td></td>
<td>zero. The counters are cleared when a unit becomes manager and with a</td>
</tr>
<tr>
<td></td>
<td>support command.</td>
</tr>
<tr>
<td></td>
<td>Range: Time Stamp. Default: 0d00:00:00</td>
</tr>
<tr>
<td>Checkpoint Message Rate</td>
<td>Number of checkpoint messages per second.</td>
</tr>
<tr>
<td>Average</td>
<td>The average is computed over the time period since the counters were</td>
</tr>
<tr>
<td></td>
<td>cleared. Range: Integer. Default: 0</td>
</tr>
<tr>
<td>Last 10-second Message Rate</td>
<td>Number of checkpoint messages per second in the last 10-second interval.</td>
</tr>
<tr>
<td>Average</td>
<td>This average is updated once every 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Range: Integer. Default: 0</td>
</tr>
<tr>
<td>Highest 10-second Message Rate</td>
<td>The highest rate recorded over a 10-second interval since the counters</td>
</tr>
<tr>
<td></td>
<td>were cleared. Range: Integer. Default: 0</td>
</tr>
</tbody>
</table>

Example:

(Switch)#show checkpoint statistics
Messages Checkpointed.....................6708
Bytes Checkpointed.........................894305
Time Since Counters Cleared..............3d 01:05:09
Checkpoint Message Rate...................0.025 msg/sec
Last 10-second Message Rate..............0 msg/sec
Highest 10-second Message Rate..........8 msg/sec

clear checkpoint statistics

This command clears the statistics for the checkpointing process.

Format: clear checkpoint statistics
Mode: Privileged EXEC
Stack Firmware Synchronization Commands

Stack firmware synchronization provides an automatic mechanism to synchronize the firmware on stack members whose firmware version differs from the version running on the stack manager. This operation can result in either an upgrade or downgrade of firmware on the mismatched stack member. However, this operation does not attempt to synchronize the stack to the latest firmware in the stack.

During firmware transfer and upgrade, operations such as code download and move management can result in undesirable behavior, such as firmware corruption on a code mismatched stack member. As a result, you receive an error if you try to access the following operations from the user interface during stack firmware synchronization:

- Move management
- Unit renumbering
- Code download
- Delete image
- Update bootcode
- Clear config

A reboot operation is allowed during stack firmware synchronization.

If the firmware is corrupted during stack firmware synchronization, manual intervention by the administrator is required to restore the switch to working condition.

During stack firmware synchronization, traps are generated on start, completion, or failure.

- Non-deterministic upgrade behavior
  
  On bootup, the image that gets synchronized depends on the one that becomes the manager. Which code version the new stack synchronizes to is fully deterministic, but might not be obvious to the user as it depends entirely on which unit becomes the manager. This might be decided by a MAC address comparison. If the administrator wants a particular version to be used by the stack, he should first ensure that this particular unit becomes stack manager.

- Bootcode Upgrades
  
  Bootcode upgrades are not initiated by the stack firmware synchronization.

**boot auto-copy-sw**

This command enables or disables stack firmware synchronization.

<table>
<thead>
<tr>
<th>Default</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>boot auto-copy-sw</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>
no boot auto-copy-sw

This command disables stack firmware synchronization.

Format  no boot auto-copy-sw
Mode    Privileged EXEC

boot auto-copy-sw trap

This command sends SNMP traps related to stack firmware synchronization.

Default  Enabled
Format    boot auto-copy-sw trap
Mode      Privileged EXEC

no boot auto-copy-sw trap

This command disables sending SNMP traps related to stack firmware synchronization.

Format  no boot auto-copy-sw trap
Mode    Privileged EXEC

boot auto-copy-sw allow-downgrade

This command enables downgrading the firmware version on the stack member if the firmware version on the manager is older than the firmware version on the member.

Default  Enabled
Format    boot auto-copy-sw allow-downgrade
Mode      Privileged EXEC

no boot auto-copy-sw allow-downgrade

This command disables downgrading the image.

Format  no boot auto-copy-sw allow-downgrade
Mode    Privileged EXEC

show auto-copy-sw

This command displays the stack firmware synchronization configuration status.

Format  show auto-copy-sw
Mode    Privileged EXEC
Example:

(Switch)#show auto-copy-sw
Stack Firmware Synchronization
Synchronization: Enabled
SNMP Trap status: Enabled
Allow Downgrade: Enabled
This chapter describes the switching commands available in the managed switch CLI.

This chapter contains the following sections:

- Port Configuration Commands
- Loopback Interface Commands
- Spanning Tree Protocol (STP) Commands
- VLAN Commands
- Double VLAN Commands
- Voice VLAN Commands
- Provisioning (IEEE 802.1p) Commands
- Protected Ports Commands
- Private Group Commands
- GARP Commands
- GVRP Commands
- GMRP Commands
- Port-Based Network Access Control Commands
- 802.1X Supplicant Commands
- Storm-Control Commands
- Port-Channel/LAG (802.3ad) Commands
- Port Mirroring
- Static MAC Filtering
- DHCP L2 Relay Agent Commands
- DHCP Client Commands
- DHCP Snooping Configuration Commands
- Dynamic ARP Inspection Commands
- IGMP Snooping Configuration Commands
- IGMP Snooping Querier Commands
- MLD Snooping Commands
- MLD Snooping Querier Commands
• **Port Security Commands**
• **LLDP (802.1AB) Commands**
• **LLDP-MED Commands**
• **Denial of Service Commands**
• **MAC Database Commands**
• **ISDP Commands**
• **Priority-Based Flow Control Commands**

The commands in this chapter are in 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.

**Port Configuration Commands**

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

**interface**

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

**Format**

```
interface <unit/slot/port>
```

**Mode**

Global Config

**interface range**

This command gives you access to a range of port interfaces, allowing the same port configuration to be applied to a set of ports.

**Format**

```
interface range <unit/slot/port>-<unit/slot/port>
```

**Mode**

Global Config

**interface vlan**

This command gives you access to the vlan virtual interface mode, which allows certain port configurations (for example, the IP address) to be applied to the VLAN interface. Type a question mark (?) after entering the interface configuration mode to see the available options.

**Format**

```
interface vlan <vlan id>
```

**Mode**

Global Config
**interface lag**

This command gives you access to the LAG (link aggregation, or port channel) virtual interface, which allows certain port configurations to be applied to the LAG interface. Type a question mark (?) after entering the interface configuration mode to see the available options.

**Note:** The IP address cannot be assigned to a LAG virtual interface. The interface must be put under a VLAN group and an IP address assigned to the VLAN group.

**Format**

```
interface lag <lag id>
```

**Mode**

Global Config

---

**auto-negotiate**

This command enables automatic negotiation on a port.

**Default**

enabled

**Format**

```
auto-negotiate
```

**Mode**

Interface Config

---

**no auto-negotiate**

This command disables automatic negotiation on a port.

**Note:** Automatic sensing is disabled when automatic negotiation is disabled.

---

**auto-negotiate all**

This command enables automatic negotiation on all ports.

**Default**

enabled

**Format**

```
auto-negotiate all
```

**Mode**

Global Config
no auto-negotiate all

This command disables automatic negotiation on all ports.

Format  no auto-negotiate all
Mode    Global Config

description

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

Format  description <description>
Mode    Interface Config

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 7000 series implementation, the MTU size is a valid integer between 1522 - 9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.

**Note:** To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see ip mtu on page 242.

Default  1518 (untagged)
Format    mtu <1518-9216>
Mode      Interface Config

no mtu

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

Format  no mtu
Mode    Interface Config

shutdown

This command disables a port.
**Switching Commands**

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

**shutdown**
This command disables a port.

<table>
<thead>
<tr>
<th>Format</th>
<th>shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**no shutdown**
This command enables a port.

<table>
<thead>
<tr>
<th>Format</th>
<th>no shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**shutdown all**
This command disables all ports.

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

<table>
<thead>
<tr>
<th>Format</th>
<th>shutdown all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

**no shutdown all**
This command enables all ports.

<table>
<thead>
<tr>
<th>Format</th>
<th>no shutdown all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

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

| Format     | speed {<100 | 10> <half-duplex | full-duplex>} |
|------------|----------------|
| Mode       | Interface Config |
Switching Commands

ProSafe Managed Switch

### speed all

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

**Format**

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

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Acceptable Values</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>100h</td>
<td>100BASE-T half duplex</td>
</tr>
<tr>
<td>100f</td>
<td>100BASE-T full duplex</td>
</tr>
<tr>
<td>10h</td>
<td>10BASE-T half duplex</td>
</tr>
<tr>
<td>10f</td>
<td>10BASE-T full duplex</td>
</tr>
</tbody>
</table>

### show port

This command displays port information.

**Format**

```
show port {<unit/slot/port> | all}
```

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</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](#) on page 134.  
|             | • **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. |
ProSafe Managed Switch

### 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><strong>Group Name</strong></td>
<td>The group name of an entry in the Protocol-based VLAN table.</td>
</tr>
<tr>
<td><strong>Group ID</strong></td>
<td>The group identifier of the protocol group.</td>
</tr>
<tr>
<td><strong>Protocol(s)</strong></td>
<td>The type of protocol(s) for this group.</td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
<td>The VLAN associated with this Protocol Group.</td>
</tr>
<tr>
<td><strong>Interface(s)</strong></td>
<td>Lists the unit/slot/port interface(s) that are associated with this Protocol Group.</td>
</tr>
</tbody>
</table>

### show port description

This command displays the port description for every port.

**Format**

```
show port description <unit/slot/port>
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>Valid slot and port number separated by forward slashes</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Shows the port description configured via the “description” command</td>
</tr>
</tbody>
</table>
**show port status**

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

**Format**

```
show port status {<unit/slot/port> | all}
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Media Type</td>
<td>“Copper” or “Fiber” for combo port.</td>
</tr>
<tr>
<td>STP Mode</td>
<td>Indicate the spanning tree mode of the port.</td>
</tr>
<tr>
<td>Physical Mode</td>
<td>Either “Auto” or fixed speed and duplex mode.</td>
</tr>
<tr>
<td>Physical Status</td>
<td>The actual speed and duplex mode.</td>
</tr>
<tr>
<td>Link Status</td>
<td>Whether the link is Up or Down.</td>
</tr>
<tr>
<td>Loop Status</td>
<td>Whether the port is in loop state or not.</td>
</tr>
<tr>
<td>Partner Flow Control</td>
<td>Whether the remote side is using flow control or not.</td>
</tr>
</tbody>
</table>

**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 238. To assign an IPv6 address to the loopback interface, see `ipv6 address` on page 357.

**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
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

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>
<tr>
<td>Received Packets</td>
<td>The number of packets received on this interface.</td>
</tr>
<tr>
<td>Sent Packets</td>
<td>The number of packets transmitted from this interface.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of this 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>IPv6 is enabled (disabled)</td>
<td>Shows whether IPv6 is enabled on the interface.</td>
</tr>
<tr>
<td>IPv6 Prefix is</td>
<td>The IPv6 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>
Spanning Tree Protocol (STP) Commands

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

**spanning-tree**

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

- **Default**: enabled
- **Format**: spanning-tree
- **Mode**: Global Config

**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

**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

**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

**spanning-tree bpdufilter default**

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

- **Default**: disabled
no spanning-tree bpdufilter default

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

Default: enabled
Format: no spanning-tree bpdufilter default
Mode: Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on the interface.

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

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface.

Format: no spanning-tree bpduflood
Mode: Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

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

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Format: no spanning-tree bpduguard
Mode: Global Config
**spanning-tree bpdumigrationcheck**

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

**Format**

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

**Mode**

Global Config

**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

**no spanning-tree configuration name**

This command resets the Configuration Identifier Name to its default.

**Format**

```
no spanning-tree configuration name
```

**Mode**

Global Config

**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

**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
**spanning-tree edgeport**

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

**Default** enabled

**Format** `spanning-tree edgeport`

**Mode** Interface Config

**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

**spanning-tree forceversion**

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

**Default** 802.1s

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

**Mode** Global Config

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

**no spanning-tree forceversion**

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

**Format** `no spanning-tree forceversion`

**Mode** Global Config
**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

**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

**spanning-tree guard**

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

**Default**

none

**Format**

spanning-tree guard { none | root | loop }

**Mode**

Interface Config

**no spanning-tree guard**

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

**Format**

no spanning-tree guard

**Mode**

Interface Config

**spanning-tree tcnguard**

This command enables the propagation of received topology change notifications and topology changes to other ports.

**Default**

disable

**Format**

spanning-tree tcnguard

**Mode**

Interface Config
no spanning-tree tcnguard

This command disables the propagation of received topology change notifications and topology changes to other ports.

Format
no spanning-tree tcnguard
Mode
Interface Config

spanning-tree max-age

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

Default
20
Format
spanning-tree max-age <6-40>
Mode
Global Config

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

spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 6 to 40.

Default
20
Format
spanning-tree max-hops <1-127>
Mode
Global Config

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
**spanning-tree mst**

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

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

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

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

**Default**

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

**Format**

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

**Mode**

Interface Config

---

**no spanning-tree mst**

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

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

If you specify **external-cost**, this command sets the external path cost for this port for mst ‘0’ instance, to the default value, i.e. a path cost value based on the Link Speed.
If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the `<mstid>` parameter, to the default value.

**Format**

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

**Mode**

Interface Config

### 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

### 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

### spanning-tree mst priority

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

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

**Default**

32768

**Format**

```
spanning-tree mst priority <mstid> <0-61440>
```

**Mode**

Global Config
no spanning-tree mst priority

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

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

Format  
no spanning-tree mst priority `<mstid>`

Mode   
Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter `<mstid>` is a number that corresponds to the desired existing multiple spanning tree instance. The vlan range can be specified as a list or as a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (“-”).

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

Mode   
Global Config

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

spanning-tree port mode

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

Default  
enabled

Format  
spanning-tree port mode

Mode   
Interface Config
no spanning-tree port mode

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

Format: no spanning-tree port mode
Mode: Interface Config

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

no spanning-tree port mode all

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

Format: no spanning-tree port mode all
Mode: Global Config

spanning-tree edgeport all

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

Format: spanning-tree edgeport all
Mode: Global Config

no spanning-tree edgeport all

This command disables Edge Port mode for all ports within the common and internal spanning tree.

Format: no spanning-tree edgeport all
Mode: Global Config

spanning-tree bpduforwarding

Normally a switch will not forward Spanning Tree Protocol (STP) BPDU packets if STP is disabled. However, if in some network setup, the user wishes to forward BDPU packets received from other network devices, this command can be used to enable the forwarding.

Default: disabled
ProSafe Managed Switch

**no spanning-tree bpduforwarding**

This command will cause the STP BPDU packets received from the network to be dropped if STP is disabled.

**Format**

```
no spanning-tree bpduforwarding
```

**Mode**

Global Config

**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><strong>Bridge Priority</strong></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><strong>Bridge Identifier</strong></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><strong>Time Since Topology Change</strong></td>
<td>Time in seconds.</td>
</tr>
<tr>
<td><strong>Topology Change Count</strong></td>
<td>Number of times changed.</td>
</tr>
<tr>
<td><strong>Topology Change</strong></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><strong>Designated Root</strong></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><strong>Root Path Cost</strong></td>
<td>Value of the Root Path Cost parameter for the common and internal spanning tree.</td>
</tr>
<tr>
<td><strong>Root Port Identifier</strong></td>
<td>Identifier of the port to access the Designated Root for the CST</td>
</tr>
<tr>
<td><strong>Root Port Max Age</strong></td>
<td>Derived value.</td>
</tr>
<tr>
<td><strong>Root Port Bridge Forward Delay</strong></td>
<td>Derived value.</td>
</tr>
<tr>
<td><strong>Hello Time</strong></td>
<td>Configured value of the parameter for the CST.</td>
</tr>
</tbody>
</table>
### 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 Hold Time</td>
<td>Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).</td>
</tr>
<tr>
<td>Bridge Max Hops</td>
<td>Bridge max-hops count for the device.</td>
</tr>
<tr>
<td>CST Regional Root Path</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>CST Regional Root Path</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>

<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>
<tr>
<td>Bridge Hold Time</td>
<td>Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).</td>
</tr>
</tbody>
</table>
**show spanning-tree interface**

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

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

**Mode**
- Privileged EXEC
- User EXEC

<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 BPDUs Transmitted</td>
<td>Spanning Tree Protocol Bridge Protocol Data Units sent.</td>
</tr>
<tr>
<td>STP BPDUs Received</td>
<td>Spanning Tree Protocol Bridge Protocol Data Units received.</td>
</tr>
<tr>
<td>RSTP BPDUs Transmitted</td>
<td>Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.</td>
</tr>
<tr>
<td>RSTP BPDUs Received</td>
<td>Rapid Spanning Tree Protocol Bridge Protocol Data Units received.</td>
</tr>
<tr>
<td>MSTP BPDUs Transmitted</td>
<td>Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.</td>
</tr>
<tr>
<td>MSTP BPDUs Received</td>
<td>Multiple Spanning Tree Protocol Bridge Protocol Data Units received.</td>
</tr>
</tbody>
</table>

**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 `<unit/slot/port>` is the desired switch port.

**Format**

```
show spanning-tree mst port detailed <mstid> <unit/slot/port>
```

**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 MST instance.</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 &quot;blocking&quot; 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>

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
The `<unit/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>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>PortForwarding 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</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 &quot;blocking&quot; state until a subsequent BPDU is received.</td>
</tr>
</tbody>
</table>
show spanning-tree mst port summary

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

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

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

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>Valid slot and port number separated by forward slashes.</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>

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.

Format: `show spanning-tree mst port summary <mstid> active`

Mode:
- Privileged EXEC
- User EXEC
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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>mstid</td>
<td>The ID of the existing MST instance.</td>
</tr>
<tr>
<td>Interface</td>
<td>unit/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>

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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSTInstance ID</td>
<td>List of multiple spanning trees IDs currently configured.</td>
</tr>
<tr>
<td>List</td>
<td></td>
</tr>
</tbody>
</table>

For each MSTID:

- Associated FIDs
- Associated VLANs

- List of forwarding database identifiers associated with this instance.
- List of VLAN IDs associated with this instance.
### Spanning Tree Configuration

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning Tree Adminmode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>Spanning Tree Version</td>
<td>Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.</td>
</tr>
<tr>
<td>BPDU Guard Mode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>BPDU Filter Mode</td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>Configuration Name</td>
<td>Identifier used to identify the configuration currently being used.</td>
</tr>
<tr>
<td>Configuration Revision Level</td>
<td>Identifier used to identify the configuration currently being used.</td>
</tr>
<tr>
<td>Configuration Digest Key</td>
<td>A generated Key used in the exchange of the BPDUs.</td>
</tr>
<tr>
<td>Configuration Format Selector</td>
<td>Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.</td>
</tr>
<tr>
<td>MST Instances</td>
<td>List of all multiple spanning tree instances configured on the switch.</td>
</tr>
</tbody>
</table>

### show spanning-tree vlan

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

**Format**

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

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Identifier</td>
<td>The VLANs associated with the selected MST instance.</td>
</tr>
<tr>
<td>Associated Instance</td>
<td>Identifier for the associated multiple spanning tree instance or “CST” if associated with the common and internal spanning tree.</td>
</tr>
</tbody>
</table>

### VLAN Commands

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

**network mgmt_vlan**

This command configures the Management VLAN ID.

**Default**

1

**Format**

```
network mgmt_vlan <1-4093>
```

**Mode**

Privileged EXEC

**no network mgmt_vlan**

This command sets the Management VLAN ID to the default.

**Format**

```
no network mgmt_vlan
```

**Mode**

Privileged EXEC

**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). The vlan-list contains VlanId's in range <1-4093>. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

**Format**

```
vlan <vlan-list>
```

**Mode**

VLAN Config

**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-list contains VlanId's in range <1-4093>. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

**Format**

```
no vlan <vlan-list>
```

**Mode**

VLAN Config
**vlan acceptframe**

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

Default all

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

Mode Interface Config

**no vlan acceptframe**

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

Format `no vlan acceptframe`

Mode Interface Config

**vlan ingressfilter**

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

Default disabled

Format `vlan ingressfilter`

Mode Interface Config

**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
vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Format: `vlan makestatic <2-4093>`
Mode: VLAN Config

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

no vlan name

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

Format: `no vlan name <1-4093>`
Mode: VLAN Config

vlan participation

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

Format: `vlan participation {exclude | include | auto} <1-4093>`
Mode: Interface Config

Participation options are:

<table>
<thead>
<tr>
<th>Participation 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. The interface 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>
### 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>Participation 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. The interface 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>

### vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

**Default**

all

**Format**

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

**Mode**

Global Config

The modes defined as follows:

<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 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.

### 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

**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

**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

**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

**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
**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

**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

**vlan protocol group**

This command adds protocol-based VLAN groups to the system. When it is created, the protocol group will be assigned a unique number (1-128) that will be used to identify the group in subsequent commands.

**Format**

```
vlan protocol group <1-128>
```

**Mode**

Global Config

**no vlan protocol group**

This command removes a protocol group.

**Format**

```
no vlan protocol group <1-128>
```

**Mode**

Global Config

**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 <1-128> <groupname>
```

**Mode**

Global Config
**no vlan protocol group name**

This command removes the name from a protocol-based VLAN groups.

**Format**

```
no vlan protocol group name <1-128>
```

**Mode**

Global Config

**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-list includes the keywords 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>|arp|ip|ipx}
```

**Mode**

Global Config

**no vlan protocol group add protocol**

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

**Format**

```
no vlan protocol group add protocol <groupid> ethertype
   {<protocol-list>|arp|ip|ipx}
```

**Mode**

Global Config

**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
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

protocol vlan group

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

Default: none
Format: protocol vlan group <groupid>
Mode: Interface Config

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

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
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

vlan pvid

This command changes the VLAN ID per interface.

Default: 1

Format: vlan pvid <1-4093>

Mode: Interface Config

no vlan pvid

This command sets the VLAN ID per interface to 1.

Format: no vlan pvid

Mode: Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The vlan-list contains VlanId's in range <1-4093>. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

Format: vlan tagging <vlan-list>

Mode: Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The vlan-list contains VlanId's in range <1-4093>. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

Format: no vlan tagging <vlan-list>

Mode: Interface Config
**vlan association subnet**

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

**Format**

```
vlan association subnet <ipaddr> <netmask> <1-4093>
```

**Mode**

VLAN Config

**no vlan association subnet**

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

**Format**

```
o vlan association subnet <ipaddr> <netmask>
```

**Mode**

VLAN Config

**vlan association mac**

This command associates a MAC address to a VLAN.

**Format**

```
vlan association mac <macaddr> <1-4093>
```

**Mode**

VLAN database

**no vlan association mac**

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

**Format**

```
o vlan association mac <macaddr>
```

**Mode**

VLAN database

**show vlan**

This command displays a list of all configured VLAN.

**Format**

```
show vlan
```

**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 (VID) associated with each VLAN. The range of 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 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>VLAN Type</td>
<td>Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).</td>
</tr>
</tbody>
</table>
show vlan <vlanid>

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

Format  
show vlan <vlanid>

Mode  
• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>There is a VLAN Identifier (VID) associated with each VLAN. The range of 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 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>VLAN Type</td>
<td>Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).</td>
</tr>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.</td>
</tr>
<tr>
<td>Current</td>
<td>The degree of participation of this port in this VLAN. The permissible values are:</td>
</tr>
<tr>
<td></td>
<td>• Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</td>
</tr>
<tr>
<td></td>
<td>• Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</td>
</tr>
<tr>
<td></td>
<td>• Autodetect - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.</td>
</tr>
<tr>
<td>Configured</td>
<td>The configured degree of participation of this port in this VLAN. The permissible values are:</td>
</tr>
<tr>
<td></td>
<td>• Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.</td>
</tr>
<tr>
<td></td>
<td>• Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.</td>
</tr>
<tr>
<td></td>
<td>• Autodetect - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.</td>
</tr>
<tr>
<td>Tagging</td>
<td>The tagging behavior for this port in this VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Tagged - Transmit traffic for this VLAN as tagged frames.</td>
</tr>
<tr>
<td></td>
<td>• Untagged - Transmit traffic for this VLAN as untagged frames.</td>
</tr>
</tbody>
</table>
**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 the VLAN ID is 1 to 3965.</td>
</tr>
<tr>
<td>VLAN Name</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>VLAN Type</td>
<td>Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).</td>
</tr>
</tbody>
</table>

**show vlan port**

This command displays VLAN port information.

**Format**  
show vlan port {<unit/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>Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.</td>
</tr>
<tr>
<td>Port VLAN ID</td>
<td>The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.</td>
</tr>
<tr>
<td>Acceptable Frame Types</td>
<td>The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.</td>
</tr>
<tr>
<td>Ingress Filtering</td>
<td>May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.</td>
</tr>
<tr>
<td>GVRP</td>
<td>May be enabled or disabled.</td>
</tr>
<tr>
<td>Default Priority</td>
<td>The 802.1p priority assigned to tagged packets arriving on the port.</td>
</tr>
</tbody>
</table>
**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 Subnet</td>
<td>The IP address assigned to each interface.</td>
</tr>
<tr>
<td>IP 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>

**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>

**Double VLAN Commands**

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

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

Default: vman
Format: dvlan-tunnel ethertype \{802.1Q | vman | custom\} \[0-65535\]
Mode: Global Config

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

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

mode dvlan-tunnel

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

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

Default: disabled
Format: mode dvlan-tunnel
Mode: Interface Config
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

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 {<unit/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>Valid slot and port number separated by forward slashes.</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 0 to 65535.</td>
</tr>
</tbody>
</table>

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 {<unit/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>Valid slot and port number separated by forward slashes.</td>
</tr>
</tbody>
</table>
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.

**voice vlan (Global Config)**

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

- **Default**: disabled
- **Format**: voice vlan
- **Mode**: Global Config

**no voice vlan (Global Config)**

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

- **Format**: no voice vlan
- **Mode**: Global Config

**voice vlan (Interface Config)**

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

- **Default**: disabled
You can configure Voice VLAN in one of three different ways:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 &lt;priority&gt; 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>

**no voice vlan (Interface Config)**

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

**voice vlan data priority**

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

**show voice vlan**

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice VLAN Interface 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 do1p 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>

**Provisioning (IEEE 802.1p) Commands**

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

**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

**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

**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.

**switchport protected (Global Config)**

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

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

**Format**

```
switchport protected <groupid> name <name>
```

**Mode**

Global Config

**no switchport protected (Global Config)**

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

**Format**

```
no switchport protected <groupid> name
```

**Mode**

Global Config

**switchport protected (Interface Config)**

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

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

Switching Commands

Default unprotected
Format switchport protected <groupid>
Mode Interface Config

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

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 &lt;groupid&gt;. If no port is configured as protected for this group, this field is blank.</td>
</tr>
</tbody>
</table>

show interfaces switchport

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

Format show interfaces switchport <unit/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 port</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 &lt;groupid&gt;.</td>
</tr>
</tbody>
</table>
Private Group Commands

This section describes commands used to configure private group and view private group configuration information.

Private group can be used to create a group of ports that can or can not share traffic to each others in the same VLAN group. The main application is to isolate a group of users from another without using VLAN.

**switchport private-group**

This command is used to assign one port or a range of ports to private group <privategroup-name> (or <private-group-id>).

The ingress traffic from a port in private group can be forwarded to other ports either in the same private group or anyone in the same VLAN that are not in a private group.

By default, a port does not belong to any private group. A port cannot be in more than one private group. An error message should return when that occurred. To change a port’s private group, first the port must be removed from its private group.

**Default**

port not associated with any group.

**Format**

switchport private-group [<privategroup-name>|<privategroup-id>]

**Mode**

Interface Config

**no switchport private group**

This command is used to remove the specified port from the given private group.

**Format**

no switchport private-group [<privategroup-name>|<privategroup-id>]

**Mode**

Interface Config

**private-group name**

This command is used to create a private group with name <private-group-name>. The name string can be up to 24 bytes of non-blank characters. The total number of private groups is 192 such that the valid range for the ID is <1-192>.

The <private-group-id> field is optional. If not specified, a group id not used will be assigned automatically.

The mode can be either "isolated" or “community”. When in “isolated” mode, the member port in the group cannot forward its egress traffic to any other members in the same group. By
default, the mode is “community” mode that each member port can forward traffic to other members in the same group, but not to members in other groups.

**Format**

```
private-group name <privategroup-name> [groupid] [mode {community|isolated}]
```

**Mode**

Global Config

### no private-group name

This command is used to remove the specified private group.

**Format**

```
private-group name <privategroup-name>
```

**Mode**

Global Config

### show private-group

This command displays the private groups' information.

**Format**

```
show private-groupname [<private-group-name>|<private-group-id>|port <unit/slot/port>]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Port VLANID</td>
<td>The VLAN ID associated with the port.</td>
</tr>
<tr>
<td>Private Group ID</td>
<td>Total number of private groups is 192.</td>
</tr>
<tr>
<td>Private Group Name</td>
<td>The name string can be up to 24 bytes of non-blank characters</td>
</tr>
<tr>
<td>Private Group Mode</td>
<td>The mode can be either “isolated” or “community”.</td>
</tr>
</tbody>
</table>

## GARP Commands

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

### set garp timer join

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

**Default**

20  

**Format**

`set garp timer join <10-100>`

**Mode**

- Interface Config
- Global Config

**no set garp timer join**

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

**Format**

`no set garp timer join`

**Mode**

- Interface Config
- Global Config

**set garp timer leave**

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

**Default**

60  

**Format**

`set garp timer leave <20-600>`

**Mode**

- Interface Config
- Global Config

**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

**set garp timer leaveall**

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

Default 1000
Format set garp timer leaveall <200-6000>
Mode • Interface Config
       • Global Config

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

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>

**GVRP Commands**

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

**Note:** If GVRP is disabled, the system does not forward GVRP messages.
set gvrp adminmode

This command enables GVRP on the system.

Default: disabled
Format: set gvrp adminmode
Mode: Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format: no set gvrp adminmode
Mode: Privileged EXEC

set gvrp interfacemode

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

Default: disabled
Format: set gvrp interfacemode
Mode: • Interface Config
• Global Config

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

show gvrp configuration

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

Format: show gvrp configuration {<unit/slot/port> | all}
Mode: • Privileged EXEC
• User EXEC
Interface

Valid slot and port number separated by forward slashes.

Join Timer

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

Leave Timer

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

LeaveAll Timer

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

Port GVMRP Mode

The GVRP 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.

GMRP Commands

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

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

```
set gmrp adminmode
```

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

Default: disabled

Format: set gmrp adminmode

Mode: Privileged EXEC
**no set gmrp adminmode**

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

**Format**

no set gmrp adminmode

**Mode**

Privileged EXEC

**set gmrp interfacemode**

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

**Default**

disabled

**Format**

set gmrp interfacemode

**Mode**

- Interface Config
- Global Config

**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

**show gmrp configuration**

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

**Format**

show gmrp configuration {<unit/slot/port> | all}

**Mode**

- Privileged EXEC
- User EXEC
### Interface

**Term** | **Definition**
---|---
Interface | The unit/slot/port of the interface that this row in the table describes.

### Join Timer

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

### Leave Timer

**Term** | **Definition**
---|---
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

**Term** | **Definition**
---|---
LeaveAll Timer | This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain uninterrupted service. 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

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

### show mac-address-table gmrp

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

**Format** | show mac-address-table gmrp
---|---
**Mode** | Privileged EXEC

### Term

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Address</td>
<td>A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as 8 bytes.</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>
<tr>
<td>Interfaces</td>
<td>The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).</td>
</tr>
</tbody>
</table>

### Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (802.1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.
**clear dot1x statistics**

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

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

**Mode**
Privileged EXEC

**clear radius statistics**

This command is used to clear all RADIUS statistics.

**Format**
clear radius statistics

**Mode**
Privileged EXEC

**dot1x guest-vlan**

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

**Default**
disabled

**Format**
dot1x guest-vlan <vlan-id>

**Mode**
Interface Config

**no dot1x guest-vlan**

This command disables Guest VLAN on the interface.

**Default**
disabled

**Format**
no dot1x guest-vlan

**Mode**
Interface Config

**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 <unit/slot/port>

**Mode**
Privileged EXEC

**dot1x mac-auth-bypass**

This command enables MAC-Based Authentication Bypass (MAB) for 802.1x-unaware clients. MAB provides 802.1x-unaware clients controlled access to the network using the
devices’ MAC address as an identifier. This requires that the known and allowable MAC address and corresponding access rights be pre-populated in the authentication server. MAB works only when the port control mode of the port is MAC-based.

**Format**

```
dot1x mac-auth-bypass
```

**Mode**

```
Interface Config
```

**no dot1x mac-auth-bypass**

This command disables MAB for 802.1x-unaware clients.

**Format**

```
no dot1x mac-auth-bypass
```

**Mode**

```
Interface Config
```

**dot1x max-req**

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

**Default**

2

**Format**

```
dot1x max-req <count>
```

**Mode**

```
Interface Config
```

**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
```

**dot1x max-users**

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

**Default**

16

**Format**

```
dot1x max-users <count>
```

**Mode**

```
Interface Config
```
no dot1x max-users

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

Format: `no dot1x max-req`
Mode: Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified port. Select `force-unauthorized` to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select `force-authorized` to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select `auto` to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

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

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

dot1x port-control all

This command sets the authentication mode to use on all ports. Select `force-unauthorized` to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select `force-authorized` to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select `auto` to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

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

dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is “auto” or “mac-based”. If the control mode is not “auto” or “mac-based”, an error will be returned.

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

dot1x re-authentication

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

Default   disabled
Format     dot1x re-authentication
Mode       Interface Config

no dot1x re-authentication

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

Format     no dot1x re-authentication
Mode       Interface Config

dot1x system-auth-control

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

Default   disabled
Format     dot1x system-auth-control
Mode       Global Config
no dot1x system-auth-control

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

**Format**

```
no dot1x system-auth-control
```

**Mode**

Global Config

---

**dot1x timeout**

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

<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 re-authentication 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
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

dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with that port. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (4093 for 7000 series). 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

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

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> {<unit/slot/port> | all}

Mode: Global Config

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> {<unit/slot/port> | all}

Mode: Global Config
**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 [unit/slot/port]
```

**Mode**

Global Config

**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.

**Format**

```
dot1x dynamic-vlan enable
```

**Mode**

Global Config

**Default**

Disabled

**no dot1x dynamic-vlan enable**

Use this command to disable the switch from creating VLANs dynamically when a RADIUS assigned VLAN does not exist in the switch.

**Format**

```
no dot1x dynamic-vlan enable
```

**Mode**

Global Config

**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 troubleshoot 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.

**Format**

```
dot1x system-auth-control monitor
```

**Mode**

Global Config

**Default**

Disabled

**no dot1x system-auth-control monitor**

Use this command to disable the 802.1X monitor on the switch.

**Format**

```
no dot1x system-auth-control monitor
```

**Mode**

Global Config
**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**

```plaintext
show dot1x authentication-history {unit/slot/port | all} [failedauth-only] [detail]
```

**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>

**show authentication methods**

This command displays information about the authentication methods.

**Format**

```plaintext
show authentication methods
```

**Mode**

Privileged EXEC

The following is an example of this command:

```
Login Authentication Method Lists

Console_Default: None
Network_Default:Local
Enable Authentication Lists

Console_Default: Enable None
Network_Default:Enable
Line Login Method List Enable Method Lists

Console Console_Default Console_Default
Telnet Network_Default Network_Default
SSH Network_Default Network_Default
http : Local
https : Local
dot1x :
```
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 {<unit/slot/port> | all} | detail <unit/slot/port> | statistics <unit/slot/port>}

Mode

Privileged EXEC

If you do not use the optional parameters <unit/slot/port> or <vlanid>, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

<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>
<tr>
<td>Dynamic VLAN Creation Mode</td>
<td>Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.</td>
</tr>
<tr>
<td>Monitor Mode</td>
<td>Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface whose configuration is displayed.</td>
</tr>
<tr>
<td>Control Mode</td>
<td>The configured control mode for this port. Possible values are force-unauthorized</td>
</tr>
<tr>
<td>Operating Control Mode</td>
<td>The control mode under which this port is operating. Possible values are authorized</td>
</tr>
<tr>
<td>Reauthentication Enabled</td>
<td>Indicates whether re-authentication is enabled on this port.</td>
</tr>
<tr>
<td>Port Status</td>
<td>Indicates whether the port is authorized or unauthorized. Possible values are authorized</td>
</tr>
</tbody>
</table>
If you use the optional parameter `detail <unit/slot/port>`, the detailed dot1x configuration for the specified port is displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The interface whose configuration is displayed.</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.</td>
</tr>
<tr>
<td>PAE Capabilities</td>
<td>The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.</td>
</tr>
<tr>
<td>Control Mode</td>
<td>The configured control mode for this port. Possible values are force-unauthorized</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. When MAC-based authentication is enabled on the port, this parameter is deprecated.</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. When MAC-based authentication is enabled on the port, this parameter is deprecated.</td>
</tr>
<tr>
<td>Quiet Period</td>
<td>The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.</td>
</tr>
<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>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 Id 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>
</tbody>
</table>
### ProSafe Managed Switch

**The show dot1x detail <unit/slot/port> command will display the following MAC-based dot1x fields if the port-control mode for that specific port is MAC-based.**

For each client authenticated on the port, the `show dot1x detail <unit/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>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>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>

**The show dot1x detail <unit/slot/port> command will display the following MAC-based dot1x fields 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 <unit/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>
<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>

**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 {<unit/slot/port> | all}
```

**Mode**

Privileged EXEC
show dot1x users

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

Format  show dot1x users <unit/slot/port>
Mode    Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients Authenticated using Monitor Mode</td>
<td>Indicates the number of the Dot1x clients authenticated using Monitor mode.</td>
</tr>
<tr>
<td>Clients Authenticated using Dot1x</td>
<td>Indicates the number of Dot1x clients authenticated using 802.1x authentication process.</td>
</tr>
<tr>
<td>Logical Interface</td>
<td>The logical port number associated with a client.</td>
</tr>
<tr>
<td>Interface</td>
<td>The physical port to which the supplicant is associated.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name used by the client to authenticate to the server.</td>
</tr>
<tr>
<td>Supplicant MAC Address</td>
<td>The supplicant device MAC address.</td>
</tr>
<tr>
<td>Session Time</td>
<td>The time since the supplicant is logged on.</td>
</tr>
<tr>
<td>Filter ID</td>
<td>Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN assigned to the port.</td>
</tr>
<tr>
<td>VLAN Assigned</td>
<td>The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the PVID of the port was that VLAN ID.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.</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 and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.</td>
</tr>
</tbody>
</table>
802.1X Supplicant Commands

802.1X ("dot1x") supplicant functionality is on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

**dot1x pae**

Use this command to set the port's dot1x role. The port can serve as either a supplicant or an authenticator.

**Format**

dot1x pae {supplicant | authenticator}

**Mode**

Interface Config

**dot1x supplicant port-control**

Use this command to set 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>Term</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>

**no dot1x supplicant port-control**

Use this command to set the port-control mode to the default, auto.

**Default**

Auto

**Format**

no dot1x supplicant port-control

**Mode**

Interface Config
**dot1x supplicant max-start**

Use this command to configure 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

**no dot1x supplicant max-start**

Use this command to set the max-start value to the default.

- **Format**: `no dot1x supplicant max-start`
- **Mode**: Interface Config

**dot1x supplicant timeout start-period**

Use this command to configure 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

**no dot1x supplicant timeout start-period**

Use this command to set the start-period value to the default.

- **Format**: `no dot1x supplicant timeout start-period`
- **Mode**: Interface Config

**dot1x supplicant timeout held-period**

Use this command to configure the held period timer interval to wait for the next authentication on previous authentication fail.

- **Default**: 30 seconds
- **Format**: `dot1x supplicant timeout held-period <1-65535 seconds>`
- **Mode**: Interface Config
no dot1x supplicant timeout held-period
Use this command to set the held-period value to the default value.

Format: no dot1x supplicant timeout held-period
Mode: Interface Config

dot1x supplicant timeout auth-period
Use this command to configure 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

no dot1x supplicant timeout auth-period
Use this command to set the auth-period value to the default value.

Format: no dot1x supplicant timeout auth-period
Mode: Interface Config

dot1x supplicant user
Use this command to map the given user to the port.

Format: dot1x supplicant user
Mode: Interface Config

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.

The 7000 series provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast,
multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

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

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

**storm-control broadcast**

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

<table>
<thead>
<tr>
<th>Default</th>
<th>enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>storm-control broadcast</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**no storm-control broadcast**

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

| Format   | no storm-control broadcast |
| Mode     | Interface Config |

**storm-control broadcast level**

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

Default  5
Format    storm-control broadcast level <0-100>
Mode      Interface Config

**no storm-control broadcast level**

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

Format    no storm-control broadcast level
Mode      Interface Config

**storm-control broadcast rate**

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

Default  0
Format    storm-control broadcast rate <0-14880000>
Mode      Interface Config

**no storm-control broadcast rate**

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

Format    no storm-control broadcast rate
Mode      Interface Config

**storm-control broadcast (Global)**

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

Default  disabled
no storm-control broadcast

This command disables broadcast storm recovery mode for all interfaces.

Format  no storm-control broadcast
Mode     Global Config

storm-control broadcast level (Global)

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

Default  5
Format    storm-control broadcast level <0-100>
Mode      Global Config

no storm-control broadcast level

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

Format  no storm-control broadcast level
Mode     Global Config

storm-control broadcast rate (Global)

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

Default  0
Format    storm-control broadcast rate <0-14880000>
Mode      Global Config
no storm-control broadcast rate

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

Format: no storm-control broadcast rate
Mode: Global Config

storm-control multicast

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

Default: disabled
Format: storm-control multicast
Mode: Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Format: no storm-control multicast
Mode: Interface Config

storm-control multicast level

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

Default: 5
Format: storm-control multicast level <0-100>
Mode: Interface Config

no storm-control multicast level

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

Format: no storm-control multicast level <0-100>
Mode: Interface Config
**storm-control multicast rate**

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

Default: 0

Format: `storm-control multicast rate <0-14880000>`

Mode: Interface Config

**no storm-control multicast rate**

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

Format: `no storm-control multicast rate`

Mode: Interface Config

**storm-control multicast (Global)**

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

Default: disabled

Format: `storm-control multicast`

Mode: Global Config

**no storm-control multicast**

This command disables multicast storm recovery mode for all interfaces.

Format: `no storm-control multicast`

Mode: Global Config

**storm-control multicast level (Global)**

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

Default: 5
Format: storm-control multicast level <0-100>
Mode: Global Config

no storm-control multicast level

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

Format: no storm-control multicast level
Mode: Global Config

storm-control multicast rate (Global)

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

Default: 0
Format: storm-control multicast rate <0-14880000>
Mode: Global Config

no storm-control broadcast rate

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

Format: no storm-control broadcast rate
Mode: Global Config

storm-control unicast

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

Default: disabled
no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Format: no storm-control unicast
Mode: Interface Config

storm-control unicast level

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

Default: 5
Format: storm-control unicast level <0-100>
Mode: Interface Config

no storm-control unicast level

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

Format: no storm-control unicast level
Mode: Interface Config

storm-control unicast rate

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

Default: 0
Format: storm-control unicast rate <0-14880000>
Mode: Interface Config
no storm-control unicast rate

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

**Format**

no storm-control unicast rate

**Mode**

Interface Config

**storm-control unicast (Global)**

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

**Default**

disabled

**Format**

storm-control unicast

**Mode**

Global Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces.

**Format**

no storm-control unicast

**Mode**

Global Config

**storm-control unicast level (Global)**

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

**Default**

5

**Format**

storm-control unicast level <0-100>

**Mode**

Global Config
no storm-control unicast level

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

Format  no storm-control unicast level
Mode    Global Config

storm-control unicast rate (Global)

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

Default  0
Format    storm-control unicast rate <0-14880000>
Mode     Global Config

no storm-control unicast rate

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

Format  no storm-control unicast rate
Mode    Global Config

storm-control flowcontrol

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

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

Default  disabled
Format    storm-control flowcontrol
Mode     Global Config
no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

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

Format: no storm-control flowcontrol
Mode: Global Config

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 Control 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.
- **Broadcast Storm Control Level** The broadcast storm control level. The factory default is 5%.
- **Multicast Storm Control Mode** may be enabled or disabled. The factory default is disabled.
- **Multicast Storm Control Level** The multicast storm control level. The factory default is 5%.
- **Unicast Storm Control Mode** may be enabled or disabled. The factory default is disabled.
- **Unicast Storm Control Level** The unicast storm control level. The factory default is 5%.

Use the *all* keyword to display the per-port configuration parameters for all interfaces, or specify the *unit/slot/port* to display information about a specific interface.

Format: show storm-control [all | <unit/slot/port>]
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</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>
</tbody>
</table>
Port-Channel/LAG (802.3ad) Commands

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

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>

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

addport

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

Note: Before adding a port to a port-channel, set the physical mode of the port. For more information, see speed on page 41.
deleteport (Interface Config)

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

Format: deleteport {<logical unit/slot/port>|lag <lag-group-id>}
Mode: Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical unit/slot/port number of a configured port-channel. To clear the port channels, see clear port-channel on page 530.

Format: deleteport <logical unit/slot/port>
Mode: Global Config

lacp admin key

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

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

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

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

lacp collector max-delay

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

Default: 0x8000
ProSafe Managed Switch

Switching Commands

Format: lACP collector max-delay <delay>
Mode: Interface Config

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

**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

**lACP actor admin**

Use this command to configure the LACP actor admin parameters.

**lACP actor admin key**

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

Default: Internal Interface Number of this Physical Port
Format: lACP actor admin key <key>
Mode: Interface Config

**Note:** This command is only applicable to physical interfaces.

**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

**lACP actor admin state individual**

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

Format: lACP actor admin state individual
Mode: Interface Config
**Note:** This command is only applicable to physical interfaces.

### no lACP actor admin state individual

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

**Format**

```sh
to no lACP actor admin state individual
```

**Mode**

```
Interface Config
```

### lACP actor admin state longtimeout

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

**Format**

```sh
lACP actor admin state longtimeout
```

**Mode**

```
Interface Config
```

**Note:** This command is only applicable to physical interfaces.

### no lACP actor admin state longtimeout

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

**Format**

```sh
no lACP actor admin state longtimeout
```

**Mode**

```
Interface Config
```

**Note:** This command is only applicable to physical interfaces.

### lACP actor admin state passive

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

**Format**

```sh
lACP actor admin state passive
```

**Mode**

```
Interface Config
```

**Note:** This command is only applicable to physical interfaces.
**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

**lACP actor port priority**

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

**Default**

0x80

**Format**

```
lACP actor port priority <priority>
```

**Mode**

Interface Config

**Note:** This command is only applicable to physical interfaces.

**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

**lACP actor system priority**

Use this command to configure the priority value associated with the LACP Actor's SystemID. The range for `<priority>` is 0 to 65535.

**Default**

32768

**Format**

```
lACP actor system priority <priority>
```

**Mode**

Interface Config

**Note:** This command is only applicable to physical interfaces.
**no lacp actor system priority**

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

**Format**

```
no lacp actor system priority
```

**Mode**

Interface Config

**lACP partner admin key**

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

**Default**

0x0

**Format**

```
lACP partner admin key <key>
```

**Mode**

Interface Config

---

**Note:** This command is only applicable to physical interfaces.

**no lACP partner admin key**

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

**Format**

```
no lACP partner admin key <key>
```

**Mode**

Interface Config

**lACP partner admin state individual**

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

**Format**

```
lACP partner admin state individual
```

**Mode**

Interface Config

---

**Note:** This command is only applicable to physical interfaces.

**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
**lACP Partner Admin State LLongTimeout**

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

**Format**

```plaintext
lACP partner admin state longtimeout
```

**Mode**

Interface Config

---

**Note:** This command is only applicable to physical interfaces.

**No LACP Partner Admin State LongTimeout**

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

**Format**

```plaintext
no lACP partner admin state longtimeout
```

**Mode**

Interface Config

---

**Note:** This command is only applicable to physical interfaces.

**LACP Partner Admin State Passive**

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

**Format**

```plaintext
lACP partner admin state passive
```

**Mode**

Interface Config

---

**Note:** This command is only applicable to physical interfaces.

**No LACP Partner Admin State Passive**

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

**Format**

```plaintext
no lACP partner admin state passive
```

**Mode**

Interface Config
**lacp partner port id**

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

**Default**  
0x80

**Format**  
lacp partner portid `<port-id>`

**Mode**  
Interface Config

---

**Note:** This command is only applicable to physical interfaces.

**no lacp partner port id**

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

**Format**  
no lacp partner portid

**Mode**  
Interface Config

**lacp partner port priority**

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

**Default**  
0x0

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

**Mode**  
Interface Config

---

**Note:** This command is only applicable to physical interfaces.

**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
**lacp partner system id**

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

**Default**: 00:00:00:00:00:00

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

**Mode**: Interface Config

---

**Note**: This command is only applicable to physical interfaces.

---

**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

---

**lacp partner system priority**

Use this command to configure the administrative value of the priority associated with the Partner’s System ID. The valid range for `<priority>` is 0 to 65535.

**Default**: 0x0

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

**Mode**: Interface Config

---

**Note**: This command is only applicable to physical interfaces.

---

**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
**port-channel static**

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

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td><code>port-channel static</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**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             |

**port lacpmode**

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

<table>
<thead>
<tr>
<th>Default</th>
<th>enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td><code>port lacpmode</code></td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**no port lacpmode**

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

| Format   | `no port lacpmode`           |
| Mode     | Interface Config             |

**port lacpmode enable all**

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

| Format   | `port lacpmode enable all`   |
| Mode     | Global Config                |
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

*port lacptimeout (Interface Config)*

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

**Default**

long

**Format**

port lacptimeout {actor | partner} {long | short}

**Mode**

Interface Config

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

*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

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
**port-channel adminmode**

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

**Format**

```
port-channel adminmode all
```

**Mode**

Global Config

**no port-channel adminmode**

This command disables a port-channel (LAG). This command clears every configured port-channel with the same administrative mode setting.

**Format**

```
no port-channel adminmode [all]
```

**Mode**

Global Config

**port-channel linktrap**

This command enables link trap notifications for the port-channel (LAG). The interface is a logical unit/slot/port for a configured port-channel. The option `all` enables link trap notifications for all the configured port-channels.

**Default**

enabled

**Format**

```
port-channel linktrap [<logical unit/slot/port> | all]
```

**Mode**

Global Config

**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` disables link trap notifications for all the configured port-channels.

**Format**

```
o port-channel linktrap [<logical unit/slot/port> | all]
```

**Mode**

Global Config

**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. The XSM7224S also supports enhanced hashing mode, which has the following advantages:
• MODULO-N (where N is the number of active link members in a LAG) operation based on the number of ports in the LAG
• Packet attributes selection based on the packet type: For L2 packets, source and destination MAC address are used for hash computation. For L3 packets, source IP, destination IP address, TCP/UDP ports are used.
• Non-Unicast traffic and unicast traffic is hashed using a common hash algorithm
• Excellent load balancing performance.

Default 3

Format

```
port-channel load-balance { 1 | 2 | 3 | 4 | 5 | 6 | 7}
{<unit/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>&lt;unit/slot/port&gt;</td>
<td>all Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel. &quot;All&quot; applies the command to all currently configured port-channels.</td>
</tr>
</tbody>
</table>

**no port-channel load-balance**

This command reverts to the default load balancing configuration.

Format

```
no port-channel load-balance {<unit/slot/port> | <all>}
```

Mode

Interface Config
Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;unit/slot/port&gt;</td>
<td>all Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel. &quot;All&quot; applies the command to all currently configured port-channels.</td>
</tr>
</tbody>
</table>
**port-channel name**

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

**Format**

```
port-channel name {<logical unit/slot/port> | all | <name>}
```

**Mode**

Global Config

**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

**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

**show lACP actor**

Use this command to display LACP actor attributes.

**Format**

```
show lACP actor {<unit/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 system priority assigned to the Aggregation Port.</td>
</tr>
<tr>
<td>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>
**ProSafe Managed Switch**

### show lACP partner

Use this command to display LACP partner attributes.

**Format**

```
show lACP partner {<unit/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>The value representing 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 port priority for the 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>

### show port-channel brief

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

**Format**

```
show port-channel brief
```

**Mode**

- Privileged EXEC
- User EXEC

For each port-channel the following information is displayed:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Interface</td>
<td>The unit/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>
<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>
**show port-channel**

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

**Format**

```
show port-channel
```

**Mode**

- Privileged EXEC
- User EXEC

### Static Capability

This field displays whether or not the device has static capability enabled.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Capability</td>
<td>This field displays whether or not the device has static capability enabled.</td>
</tr>
</tbody>
</table>

For each port-channel the following information is displayed:

### Term | Definition
--- | ---
Name | This field displays the name of the port-channel.
Link-State | Shows whether the link is up or down.
Mbr Ports | This field lists the ports that are members of this port-channel, in `<unit/slot/port>` notation.
Active Ports | The ports that are actively participating in the port-channel.

**show port-channel**

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

**Format**

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

**Mode**

- Privileged EXEC
- User EXEC

### Term | Definition
--- | ---
Logical Interface | Valid slot and port number separated by forward slashes.
Port-Channel Name | The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State | Indicates whether the Link is up or down.
Admin Mode | May be enabled or disabled. The factory default is enabled.
Type | The status designating whether a particular port-channel (LAG) is statically or dynamically maintained.
  - **Static** - The port-channel is statically maintained.
  - **Dynamic** - The port-channel is dynamically maintained.
### Mbr Ports
A listing of the ports that are members of this port-channel (LAG), in unit/slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).

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

### Port Speed
Speed of the port-channel port.

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

### Load Balance Option
The load balance option associated with this LAG. See `port-channel load-balance` on page 129.

---

**show port-channel system priority**

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

**Format**

```
show port-channel system priority
```

**Mode**

Privileged EXEC

---

## Port Mirroring

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

### monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). 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. Use the `destination interface <unit/slot/port>` to specify the interface to receive the monitored traffic. Use the `mode` parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

**Format**

```
monitor session <session-id> {source interface <unit/slot/port> {{rx | tx}} | destination interface <unit/slot/port> | mode}
```

**Mode**

Global Config

---

**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 <unit/slot/port> to remove the specified interface from the port monitoring session. Use the mode parameter to disable the administrative mode of the session.

**Note:** Since the current version of 7000 series software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the no monitor command.

**Format**

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

**Mode**

Global Config

**no monitor**

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

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

**Default**

enabled

**Format**

no monitor

**Mode**

Global Config

**show monitor session**

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

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

**Format**

show monitor session <session-id>

**Mode**

Privileged EXEC
Switching Commands

ProSafe Managed Switch

<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 &lt;session-id&gt;. The possible values are Enabled and Disabled.</td>
</tr>
<tr>
<td>Probe Port</td>
<td>Probe port (destination port) for the session identified with &lt;session-id&gt;. If probe port is not set then this field is blank.</td>
</tr>
<tr>
<td>Mirrored Port</td>
<td>The port, which is configured as mirrored port (source port) for the session identified with &lt;session-id&gt;. If no source port is configured for the session then 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>
</tbody>
</table>

### Static MAC Filtering

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

**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.

For example, for current 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
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

macfilter adddest

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

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

Format:  macfilter adddest <macaddr> <vlanid>

Mode:  Interface Config

no macfilter adddest

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

Format:  no macfilter adddest <macaddr> <vlanid>

Mode:  Interface Config

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.
**Switching Commands**

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

```
Format:  macfilter adddest all <macaddr> <vlanid>
Mode:    Global Config

no macfilter adddest all
```

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

```
Format:  no macfilter adddest all <macaddr> <vlanid>
Mode:    Global Config
```

```
macfilter addsrc
```

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

```
Format:  macfilter addsrc <macaddr> <vlanid>
Mode:    Interface Config
```

```
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
```

```
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

```
Format:  macfilter addsrc all <macaddr> <vlanid>
Mode:    Interface Config
```

---

ProSafe Managed Switch

---

138
Switching Commands

6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The `<vlanid>` parameter must identify a valid VLAN.

**Format**

```plaintext
macfilter addsrc all <macaddr> <vlanid>
```

**Mode**

Global Config

**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**

```plaintext
no macfilter addsrc all <macaddr> <vlanid>
```

**Mode**

Global Config

**show mac-address-table static**

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

**Format**

```plaintext
show mac-address-table static {<macaddr> <vlanid> | all}
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC Address of the static MAC filter entry.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID of the static MAC filter entry.</td>
</tr>
<tr>
<td>Source Port(s)</td>
<td>The source port filter set's slot and port(s).</td>
</tr>
</tbody>
</table>

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

**show mac-address-table staticfiltering**

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

**Format**

```plaintext
show mac-address-table staticfiltering
```

**Mode**

Privileged EXEC
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.

**dhcp l2relay**

Use this command to enable the DHCP Layer 2 Relay agent for an interface, a range of interfaces, or all interfaces. The subsequent commands mentioned in this section can be used only when the DHCP L2 relay is enabled.

**Format**

dhcp l2relay

**Modes**

- Global Config
- Interface Config

**no dhcp l2relay**

Use this command to disable the DHCP Layer 2 relay agent for an interface or range of interfaces.

**Format**

no dhcp l2relay

**Modes**

- Global Config
- Interface Config

**dhcp l2relay circuit-id vlan**

Use this parameter to set the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82. Vlan-list range is 1–4093.
Separate non-consecutive IDs with a comma (,), and do not insert spaces or zeros in between the range. Use a dash (–) for the range.

**Format**

```
dhcp l2relay circuit-id vlan <vlan-list>
```

**Mode**

Global Config

**no dhcp l2relay circuit-id vlan**

Use this parameter to clear the DHCP Option-82 Circuit ID for a VLAN.

**Format**

```
no dhcp l2relay circuit-id vlan <vlan-list>
```

**Mode**

Global Config

**dhcp l2relay remote-id vlan**

Use this parameter to set the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name). The vlan–list range is 1–4093. Separate non-consecutive IDs with a comma (,), and do not insert spaces or zeros between the range. Use a dash (–) for the range.

**Format**

```
dhcp l2relay remote-id <remote-id-string> vlan <vlan-list>
```

**Mode**

Global Config

**no dhcp l2relay remote-id vlan**

Use this parameter to clear 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

**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. vlan–list range is 1–4093. Separate non-consecutive IDs with a comma (,), and do not insert spaces or zeros between the range. Use a dash (–) for the range.

**Default**

disabled

**Format**

```
dhcp l2relay vlan <vlan-list>
```

**Mode**

Global Config
ProSafe Managed Switch

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

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

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

show dhcp l2relay all

Use this command to display 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.

(switch) #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>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>
**show dhcp l2relay interface**

Use this command to display 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.

```
(switch) #show dhcp l2relay interface all
DHCP L2 Relay is Enabled.

Interface         L2RelayMode        TrustMode
----------         -----------       --------------
1/0/2              Enabled            untrusted
1/0/4              Disabled           trusted
```

**show dhcp l2relay stats interface**

Use this command to display 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.

```
(switch) #show dhcp l2relay stats interface all
DHCP L2 Relay is Enabled.

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

**show dhcp l2relay agent-option vlan**

Use this command to display the DHCP L2 Relay Option-82 configuration specific to VLAN.

**Format**
show dhcp l2relay agent-option vlan

**Mode**
Privileged EXEC

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

```
(switch) #show dhcp l2relay agent-option vlan 5-10
DHCP L2 Relay is Enabled.

VLAN Id        L2 Relay       CircuitId           RemoteId
---------     ----------     -----------        ------------
5              Enabled         Enabled            --NULL--
```
DHCP Client Commands

DHCP Client 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.

**dhcp client vendor-id-option**

Use this command to enable 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 switch.

**Format**

```
dhcp client vendor-id-option
```

**Mode**

```
Global Config
```

**no dhcp client vendor-id-option**

Use this command to disable 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 switch.

**Format**

```
no dhcp client vendor-id-option
```

**Mode**

```
Global Config
```

**dhcp client vendor-id-option-string**

Use this command to set the DHCP Vendor Option-60 string to be included in requests transmitted to the DHCP server by the DHCP client operating in the switch.

**Format**

```
dhcp client vendor-id-option-string <string>
```

**Mode**

```
Global Config
```

**no dhcp client vendor-id-option-string**

Use this command to clear the DHCP Vendor Option-60 string.

**Format**

```
no dhcp client vendor-id-option-string
```

**Mode**

```
Global Config
```
**show dhcp client vendor-id-option**

Use this command to display 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.

```
(switch) #show dhcp client vendor-id-option
DHCP Client Vendor Identifier Option ........... Enabled
DHCP Client Vendor Identifier Option string .... Client.
```

**DHCP Snooping Configuration Commands**

This section describes commands you use to configure DHCP Snooping.

**ip dhcp snooping**

Use this command to enable DHCP Snooping globally.

**Default**  
disabled

**Format**  
```
ip dhcp snooping
```

**Mode**  
Global Config

**no ip dhcp snooping**

Use this command to disable DHCP Snooping globally.

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

**Mode**  
Global Config

**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
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

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 DCHP message.

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

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

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

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
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

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

no ip dhcp snooping binding <mac-address>

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

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

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

ip dhcp snooping limit

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

Default: 15 pps for rate limiting and 1 sec for burst interval
ProSafe Managed Switch

Format: `ip dhcp snooping limit {rate pps [burst interval seconds]}`
Mode: Interface Config

**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

**ip dhcp snooping log-invalid**

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

Default: disabled
Format: `ip dhcp snooping log-invalid`
Mode: Interface Config

**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

**ip dhcp snooping trust**

Use this command to configure the port as trusted.

Default: disabled
Format: `ip dhcp snooping trust`
Mode: Interface Config

**no ip dhcp snooping trust**

Use this command to configure the port as untrusted.

Format: `no ip dhcp snooping trust`
Mode: Interface Config
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.

Default: the source ID is the IP address
Format: ip verify source {port-security}
Mode: Interface Config

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

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>
</tbody>
</table>
**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 DCHP 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 unit/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 (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>
**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:/sai1.txt
write-delay: 5000
```

**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

**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 unit/slot/port 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>
</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>1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/13</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/14</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/15</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/16</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/17</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/18</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/19</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/0/20</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 <unit/slot/port>]

**Mode**

- Privileged EXEC
- User EXEC

**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
**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 unit/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>

**show ip source binding**

This command displays the IPSG bindings.

**Format**  
show ip source binding [{static/dynamic}] [interface unit/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</td>
</tr>
<tr>
<td></td>
<td>Snooping.</td>
</tr>
</tbody>
</table>
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.

**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

**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

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN for the entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>IP address of the interface in unit/slot/port format.</td>
</tr>
</tbody>
</table>
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

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

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

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

ip arp inspection trust

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

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

ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections.

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

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

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

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
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

arp access-list

Use this command to create an ARP ACL.

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

no arp access-list

Use this command to delete a configured ARP ACL.

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

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

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

show ip arp inspection

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

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

**Mode**  
- Privileged EXEC
- User EXEC

---

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

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

(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>

**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
Switching Commands

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 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>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>
</tr>
</tbody>
</table>

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

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 unit/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 [unit/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

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

**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
```
IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. The 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.

**set igmp**

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

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

The IGMP application supports the following activities:

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

**Default**

disabled

**Format**

set igmp

**Mode**

- Global Config
- Interface Config

**Format**

set igmp <vlanid>

**Mode**

VLAN Config

**no set igmp**

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

**Format**

no set igmp

**Mode**

- Global Config
- Interface Config

**Format**

no set igmp <vlanid>

**Mode**

VLAN Config
**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

**no set igmp interfacemode**

This command disables IGMP Snooping on all interfaces.

Format: `no set igmp interfacemode`

Mode: Global Config

**set igmp fast-leave**

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

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

Default: disabled

Format: `set igmp fast-leave`

Mode: Interface Config

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

Mode: VLAN Config

**no set igmp fast-leave**

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

Format: `no set igmp fast-leave`

Mode: Interface Config
**set igmp groupmembership-interval**

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

**Default**

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

Mode: • Interface Config
    • Global Config

**Format**

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

Mode: VLAN Config

**no set igmp groupmembership-interval**

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

**Default**

Format: `no set igmp groupmembership-interval`

Mode: • Interface Config
    • Global Config

**Format**

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

Mode: VLAN Config

**set igmp maxresponse**

This command sets the IGMP Maximum Response time for the system, or on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

**Default**

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

Mode: • Global Config
    • Interface Config
**set igmp maxresponse**

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

**Format**

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

**Mode**

VLAN Config

**no set igmp maxresponse**

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

**Format**

```
no set igmp maxresponse
```

**Mode**

• Global Config  
• Interface Config

**set igmp mcrtexpiretime**

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

**Default**

```
0
```

**Format**

```
set igmp mcrtexpiretime <0-3600>
```

**Mode**

• Global Config  
• Interface Config

**Format**

```
set igmp mcrtexpiretime <vlan_id> <0-3600>
```

**Mode**

VLAN Config

**no set igmp mcrtexpiretime**

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

**Format**

```
no set igmp mcrtexpiretime
```

**Mode**

• Global Config  
• Interface Config

**Format**

```
no set igmp mcrtexpiretime <vlan_id>
```

**Mode**

VLAN Config
**set igmp mrouter**

This command configures the VLAN ID (\(<\text{vlanId}>\)) that has the multicast router mode enabled.

**Format**

```
set igmp mrouter <vlan_id>
```

**Mode**

Interface Config

**no set igmp mrouter**

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

**Format**

```
no set igmp mrouter <vlan_id>
```

**Mode**

Interface Config

**set igmp mrouter interface**

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

**Default**

disabled

**Format**

```
set igmp mrouter interface
```

**Mode**

Interface Config

**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

**set igmp router-alert-check**

This command enables the Router-Alert validation for IGMP snooping packets

**Default**

Disabled

**Format**

```
set igmp router-alert-check
```

**Mode**

Global Config
no set igmp router-alert-check

This command disables the Router-Alert validation for IGMP snooping packets.

Format  no set igmp router-alert-check
Mode    Global Config

set igmp unknow-multicast filter

This command enables the filtering of unknown multicast packets to the VLAN. Packets with
an unknown multicast address in the destination field will be dropped. This command is
mainly used when IGMP snooping is enabled, to prevent flooding of unwanted multicast
packets to every port.

Format  set igmp unknow-multicast filter
Mode    Global Config

no set igmp unknow-multicast filter

This command disables the filtering of unknown multicast packets. Unknown multicast
packets will be flooded to all ports in the same VLAN.

Format  no set igmp unknow-multicast filter
Mode    Global Config

show igmpsnooping

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

Format  show igmpsnooping [<unit/slot/port> | <vlan_id>]
Mode    Privileged EXEC

When the optional arguments <unit/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>
</tbody>
</table>
When you specify the `<unit/slot/port>` values, the following information appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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 a value for `<vlan_id>`, the following information appears:

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

Switching Commands

167
**show igmpsnooping mrouter interface**

This command displays information about statically configured ports.

**Format**
show igmpsnooping mrouter interface <unit/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>Multicast Router Attached</td>
<td>Indicates whether multicast router is statically enabled on the interface.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The list of VLANs of which the interface is a member.</td>
</tr>
</tbody>
</table>

**show igmpsnooping mrouter vlan**

This command displays information about statically configured ports.

**Format**
show igmpsnooping mrouter vlan <unit/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>

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

**set igmp querier**

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

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

---

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

---

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

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>set igmp querier [(&lt;vlan-id&gt;)] [address ipv4_address]</td>
</tr>
</tbody>
</table>
| Mode        | • Global Config  
              • VLAN Mode |

**no set igmp querier**

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

| Format      | no set igmp querier [\(<vlan-id>\)] [address] |
| Mode        | • Global Config  
              • VLAN Mode |
set igmp querier query-interval

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

Default: disabled
Format: set igmp querier query-interval <1-18000>
Mode: Global Config

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

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

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

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
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

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

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

show igmpsnooping querier

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

Format: show igmpsnooping querier [{detail | vlan <vlanid>}] 
Mode: Privileged EXEC

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

<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>
</tbody>
</table>
When you specify a value for `<vlanid>`, the following additional information appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

**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.
**set mld**

Use this command to enable 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**  
**Format**  
**Mode**

**no set mld**

Use this command to disable MLD Snooping on the system.

**Format**  
**Mode**

**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**  
**Format**  
**Mode**
no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Format:  

Mode:  

set mld fast-leave

Use this command to enable MLD Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving and MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

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

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

Default:  disabled

Format:  

Mode:  

no set mld fast-leave

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

Format:  

Mode:  

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

**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

**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

**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

**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, that is, no expiration.

**Default**: 0  
**Format**: set mld mcrtexpiretime vlanid 0-3600  
**Mode**:  
- Global Config  
- Interface Config

### 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

### 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

### 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

### 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
**ProSafe Managed Switch**

**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

**show mldsnooping**

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

**Format**

```
show mldsnooping [unit/slot/port | vlanid]
```

**Mode**

Privileged EXEC

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

<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</td>
<td>Interfaces on which MLD Snooping is enabled.</td>
</tr>
<tr>
<td>Snooping</td>
<td></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</td>
<td>VLANs on which MLD Snooping is enabled.</td>
</tr>
<tr>
<td>Snooping</td>
<td></td>
</tr>
</tbody>
</table>

When you specify the `unit/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</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>
<tr>
<td>Expiration Time</td>
<td></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>

**show mldsnooping mrouter interface**

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

Format: `show mldsnooping mrouter interface unit/slot/port`

Mode: Privileged EXEC

<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>

**show mldsnooping mrouter vlan**

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

Format: `show mldsnooping mrouter vlan unit/slot/port`

Mode: Privileged EXEC

<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>

**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
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.

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
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

set mld querier query_interval

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

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

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

set mld querier timer expiry

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

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

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
**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

**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

**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 `vlanid` 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 `vlanid`, 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 “Querier” or “Non-Querier” state. When the switch is in Querier state, it will send out periodic general queries. When in Non-Querier state, it will wait for moving to Querier state and does not send out any queries.</td>
</tr>
<tr>
<td>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 queriers 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.

**Port Security Commands**

This section describes the commands 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 port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

---

**Note:** To enable the SNMP trap specific to port security, see `snmp-server enable traps violation` on page 631.
**port-security**

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

**Default**

disabled

**Format**

port-security

**Mode**

- Global Config
- Interface Config

**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

**port-security max-dynamic**

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

**Default**

600

**Format**

port-security max-dynamic <maxvalue>

**Mode**

Interface Config

**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

**port-security max-static**

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

**Default**

20

**Format**

port-security max-static <maxvalue>

**Mode**

Interface Config

---

ProSafe Managed Switch

Switching Commands

183
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

port-security mac-address

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

Format: port-security mac-address <mac-address> <vid>
Mode: Interface Config

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

port-security mac-address move

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

Format: port-security mac-address move
Mode: Interface Config

show port-security

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

Format: show port-security [{<unit/slot/port> | all}]
Mode: Privileged EXEC

<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>
</tbody>
</table>
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 Interface.</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>
</tbody>
</table>

**show port-security dynamic**

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

**Format**

show port-security dynamic <unit/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>

**show port-security static**

This command displays the statically locked MAC addresses for port.

**Format**

show port-security static <unit/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 statically locked MAC.</td>
</tr>
</tbody>
</table>

**show port-security violation**

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

**Format**

show port-security violation <unit/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 discarded packet on locked port.</td>
</tr>
</tbody>
</table>
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.

**lldp transmit**

Use this command to enable the LLDP advertise capability.

**Default** enabled

**Format** lldp transmit

**Mode** Interface Config

**no lldp transmit**

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

**Format** no lldp transmit

**Mode** Interface Config

**lldp receive**

Use this command to enable the LLDP receive capability.

**Default** enabled

**Format** lldp receive

**Mode** Interface Config

**no lldp receive**

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

**Format** no lldp receive

**Mode** Interface Config

**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
Switching Commands

ProSafe Managed Switch

range is 2-10. The `<reinit-seconds>` is the delay before re-initialization, and the range is 1-0 seconds.

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

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

Mode
Global Config

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

lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use `sys-name` to transmit the system name TLV. To configure the system name, see `snmp-server` on page 628. 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 40

Default
all optional TLVs are included

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

Mode
Interface Config

no lldp transmit-tlv

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

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

Mode
Interface Config
**lldp transmit-mgmt**

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

Default: enabled

Format: `lldp transmit-mgmt`

Mode: Interface Config

**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

**lldp notification**

Use this command to enable remote data change notifications.

Default: disabled

Format: `lldp notification`

Mode: Interface Config

**no lldp notification**

Use this command to disable notifications.

Default: disabled

Format: `no lldp notification`

Mode: Interface Config

**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
**no lldp notification-interval**

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

**Format**

no lldp notification-interval

**Mode**

Global Config

---

**clear lldp statistics**

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

**Format**

clear lldp statistics

**Mode**

Privileged Exec

---

**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

---

**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 re-initialization, 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>

---

**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 \(<unit/slot/port> | all\)

**Mode**

Privileged Exec
ProSafe Managed Switch

### 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 {<unit/slot/port> | all}
```

**Mode**

Privileged Exec

<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>

The table contains the following column headings:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface in unit/slot/port format.</td>
</tr>
<tr>
<td>Transmit Total</td>
<td>Total number of LLDP packets transmitted on the port.</td>
</tr>
<tr>
<td>Receive 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>
</tbody>
</table>
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 {<unit/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>
<tr>
<td>Chassis ID</td>
<td>The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the 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>
</tbody>
</table>

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

(switch) #show lldp remote-device all

LLDP Remote Device Summary

Local Interface RemID Chassis ID Port ID System Name
------- ------ ------------------ ------------------ -------------
0/1 0/2 0/3 0/4 0/5 0/6 0/7 2 00:FC:E3:90:01:0F 00:FC:E3:90:01:11
0/7 3 00:FC:E3:90:01:0F 00:FC:E3:90:01:12
0/7 4 00:FC:E3:90:01:0F 00:FC:E3:90:01:13
Switching Commands

0/7        5       00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7        1       00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7        6       00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit

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 <unit/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 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 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</td>
<td>Indicates the primary function(s) of the device.</td>
</tr>
<tr>
<td>Capabilities Supported</td>
<td>Shows which of the supported system capabilities are enabled.</td>
</tr>
<tr>
<td>Management Address</td>
<td>For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.</td>
</tr>
<tr>
<td>Time To Live</td>
<td>The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the command.
(Switch) #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

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 {<unit/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 unit/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>

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 <unit/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>
<tr>
<td>Port ID Subtype</td>
<td>The type of port on the local device.</td>
</tr>
</tbody>
</table>
ProSafe Managed Switch

Switching Commands

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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 local device.</td>
</tr>
<tr>
<td>System Description</td>
<td>Describes the local 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.</td>
</tr>
<tr>
<td>System Capabilities Supported</td>
<td>Indicates the primary function(s) of the device.</td>
</tr>
<tr>
<td>System Capabilities Enabled</td>
<td>Shows which of the supported system capabilities are enabled.</td>
</tr>
<tr>
<td>Management Address</td>
<td>The type of address and the specific address the local LLDP agent uses to send and receive information.</td>
</tr>
</tbody>
</table>

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.

**lldp med**

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

Default: enabled

Format: `lldp med`

Mode: Interface Config

**no lldp med**

Use this command to disable MED.

Format: `no lldp med`

Mode: Interface Config
**lldp med confignotification**

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

**Default** enabled

**Format** `lldp med confignotification`

**Mode** Interface Config

**no lldp med confignotification**

Use this command to disable notifications.

**Format** `no lldp med confignotification`

**Mode** Interface Config

**lldp med transmit-tlv**

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

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

**Format**

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

**Mode** Interface Config

<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>

**no lldp med transmit-tlv**

Use this command to remove a TLV.

**Format**

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

**Mode** Interface Config
**lldp med all**

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

**Format**

```
lldp med all
```

**Mode**

Global Config

**no lldp med all**

Use this command to remove LLDP-MD on all ports.

**Format**

```
no lldp med all
```

**Mode**

Global Config

**lldp med confignotification all**

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

**Format**

```
lldp med confignotification all
```

**Mode**

Global Config

**no lldp med confignotification all**

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

**Format**

```
no lldp med confignotification all
```

**Mode**

Global Config

**lldp med faststartrepeatcount**

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

**Default**

```
3
```

**Format**

```
lldp med faststartrepeatcount [count]
```

**Mode**

Global Config

**no lldp med faststartrepeatcount**

Use this command to return to the factory default value.

**Format**

```
no lldp med faststartrepeatcount
```

**Mode**

Global Config
**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>

**no lldp med transmit-tlv**

Use this command to remove a TLV.

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

**Mode**
Global Config

**show lldp med**

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

**Format**
```
show lldp med
```

**Mode**
Privileged Exec

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Start Repeat Count</td>
<td>The number of LLDP PDUs that will be transmitted when the protocol is enabled.</td>
</tr>
<tr>
<td>Device Class</td>
<td>The local device’s MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as Class I Generic[IP Communication Controller etc.], Class II Media Conference Bridge etc.), Class III Communication [IP Telephone etc.], Class IV Network Connectivity Device, which is typically a LAN Switch, Router, IEEE 802.11 Wireless Access Point, etc.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(switch) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity

(switch) #

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. \(<unit/slot/port>\) indicates a specific physical interface. \(\text{all}\) indicates all valid LLDP interfaces.

**Format**

\(\text{show lldp med interface } \{\text{<unit/slot/port>} \mid \text{all}\}\)

**Mode**

Privileged Exec

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface in a unit/slot/port format.</td>
</tr>
<tr>
<td>Link</td>
<td>Shows whether the link is up or down.</td>
</tr>
<tr>
<td>ConfigMED</td>
<td>Shows if the LLPD-MED mode is enabled or disabled on this interface</td>
</tr>
<tr>
<td>OperMED</td>
<td>Shows if the LLPD-MED TLVs are transmitted or not on this interface</td>
</tr>
<tr>
<td>ConfigNotify</td>
<td>Shows if the LLPD-MED topology notification mode of this interface.</td>
</tr>
<tr>
<td>TLVsTx</td>
<td>Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Capabilities), 1 (Network Policy), 2 (Location), 3 (Extended PSE), 4 (Extended Pd), or 5 (Inventory).</td>
</tr>
</tbody>
</table>

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

(Switch) #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>1/0/1</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/2</td>
<td>Up</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/3</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/4</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/5</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/6</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/7</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/8</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/9</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/10</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/11</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
<tr>
<td>1/0/12</td>
<td>Down</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>0,1</td>
</tr>
</tbody>
</table>
ProSafe Managed Switch

1/0/13  Down  Disabled  Disabled  Disabled  0,1
1/0/14  Down  Disabled  Disabled  Disabled  0,1

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

--More-- or (q)uit

(Switch) #show lldp med interface 1/0/2

<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>1/0/2</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

(Routing) #

**show lldp med local-device detail**

This command displays detailed information about the LLDP data a specific interface transmits.

**Format**

```
show lldp med local-device detail <unit/slot/port>
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Application Type</td>
<td>Shows the application type. Types are unknown, voice, voicesignaling, guestvoice, guestvoicesignaling, sfotphonevoice, videoconferencing, streamingvideo, videosignaling.</td>
</tr>
<tr>
<td>Vlan ID</td>
<td>Shows the VLAN id associated with a particular policy type</td>
</tr>
<tr>
<td>Priority</td>
<td>Shows the priority associated with a particular policy type.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Shows the DSCP associated with a particular policy type.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Indicates if the policy type is unknown. In this case, the VLAN ID, Priority and DSCP are ignored.</td>
</tr>
<tr>
<td>Tagged</td>
<td>Indicates if the policy type is using tagged or untagged VLAN.</td>
</tr>
<tr>
<td>Hardware Rev</td>
<td>Shows the local hardware version.</td>
</tr>
<tr>
<td>Firmware Rev</td>
<td>Shows the local firmware version.</td>
</tr>
<tr>
<td>Software Rev</td>
<td>Shows the local software version.</td>
</tr>
<tr>
<td>Serial Num</td>
<td>Shows the local serial number.</td>
</tr>
<tr>
<td>Mfg Name</td>
<td>Shows the manufacture name.</td>
</tr>
<tr>
<td>Model Name</td>
<td>Shows the model name.</td>
</tr>
</tbody>
</table>

Example: The following shows example CLI display output for the command.
(Switch) #show lldp med local-device detail 1/0/8

LLDP MED Local Device Detail

Interface: 1/0/8

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

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

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

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

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

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
show lldp med remote-device

This command displays summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format: show lldp med remote-device {<unit/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 unit/slot/port format.</td>
</tr>
<tr>
<td>Device Class</td>
<td>The Remote device’s MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as Class I Generic [IP Communication Controller etc.], Class II Media [Conference Bridge etc.]. Class III Communication [IP Telephone etc.]), The fourth device is Network Connectivity Device, which is typically a LAN Switch/Router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point etc.</td>
</tr>
</tbody>
</table>

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

(Switch) #show lldp med remote-device all

LLDP MED Remote Device Summary

<table>
<thead>
<tr>
<th>Local</th>
<th>Interface</th>
<th>Remote ID</th>
<th>Device Class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1/0/8</td>
<td>1</td>
<td>Class I</td>
</tr>
<tr>
<td></td>
<td>1/0/9</td>
<td>2</td>
<td>Not Defined</td>
</tr>
<tr>
<td></td>
<td>1/0/10</td>
<td>3</td>
<td>Class II</td>
</tr>
<tr>
<td></td>
<td>1/0/11</td>
<td>4</td>
<td>Class III</td>
</tr>
<tr>
<td></td>
<td>1/0/12</td>
<td>5</td>
<td>Network Con</td>
</tr>
</tbody>
</table>

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 <unit/slot/port>
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Capabilities</td>
<td>Shows the supported capabilities that were received in MED TLV on this port.</td>
</tr>
<tr>
<td>Enabled capabilities</td>
<td>Shows the enabled capabilities that were enabled in MED TLV on this port.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Class</td>
<td>Shows the device class as advertised by the device remotely connected to the port.</td>
</tr>
<tr>
<td>Network Policy Information</td>
<td>Shows if network policy TLV is received in the LLDP frames on this port.</td>
</tr>
<tr>
<td>Media Application Type</td>
<td>Shows the application type. Types of applications are unknown, voice, voicesignaling, guestvoice, guestvoicesignaling, sfotphonevoice, videoconferencing, streamingvideo, videosignaling.</td>
</tr>
<tr>
<td>VLAN Id</td>
<td>Shows the VLAN id associated with a particular policy type.</td>
</tr>
<tr>
<td>Priority</td>
<td>Shows the priority associated with a particular policy type.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Shows the DSCP associated with a particular policy type.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Indicates if the policy type is unknown. In this case, the VLAN id, Priority and DSCP are ignored.</td>
</tr>
<tr>
<td>Tagged</td>
<td>Indicates if the policy type is using tagged or untagged VLAN.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>Shows the hardware version of the remote device.</td>
</tr>
<tr>
<td>Firmware Revision</td>
<td>Shows the firmware version of the remote device.</td>
</tr>
<tr>
<td>Software Revision</td>
<td>Shows the software version of the remote device.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Shows the serial number of the remote device.</td>
</tr>
<tr>
<td>Manufacturer Name</td>
<td>Shows the manufacture name of the remote device.</td>
</tr>
<tr>
<td>Model Name</td>
<td>Shows the model name of the remote device.</td>
</tr>
<tr>
<td>Asset ID</td>
<td>Shows the asset id of the remote device.</td>
</tr>
<tr>
<td>Sub Type</td>
<td>Shows the type of location information.</td>
</tr>
<tr>
<td>Location Information</td>
<td>Shows the location information as a string for a given type of location id</td>
</tr>
<tr>
<td>Device Type</td>
<td>Shows the remote device’s PoE device type connected to this port.</td>
</tr>
<tr>
<td>Available</td>
<td>Shows the remote port’s PSE power value in tenths of a watt.</td>
</tr>
<tr>
<td>Source</td>
<td>Shows the remote port's PSE power source.</td>
</tr>
<tr>
<td>Priority</td>
<td>Shows the remote port's PSE priority.</td>
</tr>
<tr>
<td>Required</td>
<td>Shows the remote port's PD power requirement.</td>
</tr>
<tr>
<td>Source</td>
<td>Shows the remote port's PD power source.</td>
</tr>
<tr>
<td>Priority</td>
<td>Shows the remote port's PD power priority.</td>
</tr>
</tbody>
</table>

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

(Switch) #show lldp med remote-device detail 1/0/8
LLDP MED Remote Device Detail

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

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

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

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

Location
  Subtype: elin
  Info: xxx xxx xxx

Extended POE
  Device Type: pseDevice

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

Extended POE PD

  Required: 0.2 Watts
  Source: local
  Priority: low

Denial of Service Commands
This section describes the commands you use to configure Denial of Service (DoS) Control. The 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 than configured value.
- **TCP Fragment**: IP Fragment Offset = 1.
- **TCP Flag**: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port**: Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP**: Limiting the size of ICMP Ping packets.
- **SMAC = DMAC**: Source MAC address = Destination MAC address.
- **TCP Port**: Source TCP Port = Destination TCP Port.
- **UDP Port**: Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence**: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **TCP Offset**: TCP Header Offset = 1.
- **TCP SYN**: TCP Flag SYN set.
- **TCP SYN & FIN**: TCP Flags SYN and FIN set.
- **TCP FIN & URG & PSH**: TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6**: Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment**: Checks for fragmented ICMP packets.

**dos-control all**

This command enables Denial of Service protection checks globally.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>dos-control all</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

**no dos-control all**

This command disables Denial of Service prevention checks globally.

<table>
<thead>
<tr>
<th>Format</th>
<th>no dos-control all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>
**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

**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

**dos-control firstfrag**

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller than the configured value, the packets will be dropped if the mode is enabled. The default is disabled. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to 20.

Default: disabled <20>
Format: dos-control firstfrag [<0-255>]
Mode: Global Config

**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
**dos-control tcpfrag**

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

- **Default**: disabled
- **Format**: `dos-control tcpfrag`
- **Mode**: Global Config

**no dos-control tcpfrag**

This command disabled TCP Fragment Denial of Service protection.

- **Format**: `no dos-control tcpfrag`
- **Mode**: Global Config

**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

**no dos-control tcpflag**

This command sets disables TCP Flag Denial of Service protections.

- **Format**: `no dos-control tcpflag`
- **Mode**: Global Config

**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.
### ProSafe Managed Switch

**Note:** Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>dos-control l4port</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

**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>

**dos-control icmp**

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled &lt;512&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>dos-control icmp [&lt;0-1023&gt;]</td>
</tr>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

**no dos-control icmp**

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

<table>
<thead>
<tr>
<th>Format</th>
<th>no dos-control icmp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

**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.

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

**no dos-control smacdmac**

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

Format: no dos-control smacdmac
Mode: Global Config

**dos-control tcppport**

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

Default: disabled
Format: dos-control tcppport
Mode: Global Config

**no dos-control tcppport**

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

Format: no dos-control smacdmac
Mode: Global Config

**dos-control udppport**

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

Default: disabled
Format: dos-control udppport
Mode: Global Config
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

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

no dos-control tcpflagseq

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

Format: no dos-control tcpflagseq
Mode: Global Config

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

no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format: no dos-control tcpoffset
Mode: Global Config
### 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

### 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

### dos-control tcpsynfin

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

### no dos-control tcpsynfin

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

- **Format**: `no dos-control tcpsynfin`
- **Mode**: Global Config

### dos-control tcpfinurgpsh

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
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

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 <0-16384>
Mode: Global Config

no dos-control icmpv4

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

Format: no dos-control icmpv4
Mode: Global Config

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 <0-16384>
Mode: Global Config
no dos-control icmpv6

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

Format  
Mode  

**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  
Format  
Mode  

no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format  
Mode  

**show dos-control**

This command displays Denial of Service configuration information.

Format  
Mode  

---

**Note:** Not all messages below are available in all 7000series managed switches.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Fragment Mode</td>
<td>May be enabled or disabled. The factory default is disabled.</td>
</tr>
<tr>
<td>Min TCP Hdr Size</td>
<td>The factory default is 20.</td>
</tr>
<tr>
<td>ICMP Mode</td>
<td>May be enabled or disabled. The factory default is disabled.</td>
</tr>
</tbody>
</table>
MAC Database Commands

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

*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.

<table>
<thead>
<tr>
<th>Default</th>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bridge aging-time <code>&lt;10-1,000,000&gt;</code></td>
<td>Global Config</td>
</tr>
</tbody>
</table>
### Switching Commands

**no bridge aging-time**

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

**Format**  
no bridge aging-time

**Mode**  
Global Config

**show forwardingdb agetime**

This command displays the timeout for address aging.

**Default**  
300s

**Format**  
show forwardingdb agetime

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Aging Timeout</td>
<td>This parameter displays the address aging timeout for the associated forwarding database.</td>
</tr>
</tbody>
</table>

**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>MAC Address</td>
<td>A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as a MAC address and VLAN ID combination of 8 bytes.</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>Component</td>
<td>The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.</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>
<tr>
<td>Forwarding Interfaces</td>
<td>The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.</td>
</tr>
</tbody>
</table>
show mac-address-table stats

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

Format show mac-address-table stats
Mode Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max MFDB Table Entries</td>
<td>The total number of entries that can possibly be in the Multicast Forwarding Database table.</td>
</tr>
<tr>
<td>Most MFDB Entries Since Last Reset</td>
<td>The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.</td>
</tr>
<tr>
<td>Current Entries</td>
<td>The current number of entries in the MFDB.</td>
</tr>
</tbody>
</table>

**ISDP Commands**

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

**isdp run**

This command enables ISDP on the switch.

Default Enabled
Format isdp run
Mode Global Config

**no isdp run**

This command disables ISDP on the switch.

Format no isdp run
Mode Global Config

**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
Switching Commands

ProSafe Managed Switch

**isdp holdtime**

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

Default: 30 seconds

Format: `isdp holdtime <10-255>`

Mode: Global Config

**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

**no isdp advertise-v2**

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

Format: `no isdp advertise-v2`

Mode: Global Config

**isdp enable**

This command enables ISDP on the interface.

Default: Enabled

Format: `isdp enable`

Mode: Interface Config

**no isdp enable**

This command disables ISDP on the interface.

Format: `no isdp enable`

Mode: Interface Config
clear isdp counters

This command clears ISDP counters.

Format clear isdp counters
Mode Privileged EXEC

clear isdp table

This command clears entries in the ISDP table.

Format clear isdp table
Mode Privileged EXEC

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>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>
</tbody>
</table>
| Device ID Format Capability | Indicates the Device ID format capability of the device.  
  • `serialNumber` indicates that the device uses a serial number as the format for its Device ID.  
  • `macAddress` indicates that the device uses a Layer 2 MAC address as the format for its Device ID.  
  • `other` indicates that the device uses its platform-specific format as the format for its Device ID.                                                                                                                                                                      |
| Device ID Format           | Indicates the Device ID format of the device.  
  • `serialNumber` indicates that the value is in the form of an ASCII string containing the device serial number.  
  • `macAddress` indicates that the value is in the form of a Layer 2 MAC address.  
  • `other` indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains `serialNumber` appended/ prepended with system name.                                                                                     |
**show isdp interface**

This command displays ISDP settings for the specified interface.

**Format**

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

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>ISDP mode enabled/disabled status for the interface(s).</td>
</tr>
</tbody>
</table>

**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>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>Capability</td>
<td>ISDP Functional Capabilities advertised by the neighbor.</td>
</tr>
</tbody>
</table>

**show isdp neighbors**

This command displays the list of neighboring devices.

**Format**

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

**Mode**

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

(Switch) #show isdp neighbors detail

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

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>
</tbody>
</table>
Switching Commands

### ProSafe Managed Switch

#### 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

#### 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

### Priority-Based Flow Control Commands

Ordinarily, when flow control is enabled on a physical link, it applies to all traffic on the link. When congestion occurs, the hardware sends pause frames that temporarily suspend traffic flow. Pausing traffic helps prevent buffer overflow and dropped frames.

Priority-based flow control provides a way to distinguish which traffic on physical link is paused when congestion occurs, based on the priority of the traffic. An interface can be configured to pause only high priority (i.e., loss-sensitive) traffic when necessary to prevent

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>ISDP Table Full</td>
<td>Number of times a neighbor entry was not added to the table due to a full database</td>
</tr>
<tr>
<td>ISDP IP Address Table Full</td>
<td>Displays the number of times a neighbor entry was added to the table without an IP address.</td>
</tr>
</tbody>
</table>
dropped frames, while allowing traffic that has greater loss tolerance to continue to flow on the interface.

Priorities are differentiated by the priority field of the IEEE 802.1Q VLAN header, which identifies an IEEE 802.1p priority value. In NETGEAR Managed Switch, these priority values must be mapped to internal class-of-service (CoS) values.

To enable priority-based flow control for a particular CoS value on an interface:

- Ensure that VLAN tagging is enabled on the interface so that the 802.1p priority values are carried through the network.
- Ensure that 802.1p priority values are mapped to IEEE 802.1Q CoS values.
- Use the datacenter-bridging priority-flow-control mode command to enable priority-based flow control on the interface.
- Use the datacenter-bridging priority-flow-control priority command to specify the CoS values that should be paused ("no-drop") due to greater loss sensitivity. Unless configured as "no-drop," all CoS priorities are considered nonpausable ("drop") when priority-based flow control is enabled.

When priority-flow-control is disabled, the interface defaults to the IEEE 802.3x flow control setting for the interface. When priority-based flow control is enabled, the interface will not pause any CoS unless there is at least one no-drop priority.

**datacenter-bridging priority-flow-control mode on**

Use this command to enable priority-based flow control on an interface.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Interface Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**no datacenter-bridging priority-flow-control mode**

Use this command to disable priority flow control on an interface.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Interface Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**datacenter-bridging priority-flow-control priority**

Use this command to specify the priority group(s) that should be paused when necessary to prevent dropped frames; i.e., the group to receive priority flow control. This configuration has no effect on interfaces not enabled for priority flow control.

VLAN tagging must be enabled to carry the 802.1p value through the network. The number of lossless priorities supported on XSM7224S is 2.
Additionally, the mapping of class-of-service levels to 802.1p priority values to must be set to one-to-one.

Format
```
datacenter-bridging priority-flow-control priority
priority-list {drop | no-drop}
```

Mode
Interface Config

Default
drop

**show datacenter-bridging priority-flow-control**

This command displays a summary of the priority flow control configuration for a specified interface or all interfaces.

Format
```
show datacenter-bridging priority-flow-control [interface
<unit/slot/port>]
```

Mode
Privileged EXEC

(Switch) #show datacenter-bridging priority-flow-control

<table>
<thead>
<tr>
<th>Port</th>
<th>Drop</th>
<th>No-Drop</th>
<th>State</th>
<th>Priorities</th>
<th>Priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>1-4,7</td>
<td>5,6</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/0/2</td>
<td>1-4,6-7</td>
<td>5</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/0/48</td>
<td>1-4,7</td>
<td>5,6</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This chapter contains the following sections:

- About MVR
- MVR Commands

**About MVR**

Internet Group Management Protocol (IGMP) Layer 3 is widely used for IPv4 network multicasting. In Layer 2 networks, IGMP uses resources inefficiently. For example, a Layer 2 switch multicasts traffic to all ports, even if there are receivers connected to only a few ports.

To address this problem, the IGMP Snooping protocol was developed. The problem still appears, though, when receivers are in different VLANs.

MVR is intended to solve the problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over a Layer 2 network in conjunction with IGMP snooping.

**MVR Commands**

**mvr**

This command enables MVR.

<table>
<thead>
<tr>
<th>Format</th>
<th>mvr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
<tr>
<td></td>
<td>Interface Config</td>
</tr>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
**no mvr**

This command disables MVR.

**Format**

```
no mvr
```

**Mode**

- Global Config
- Interface Config

**mvr group**

This command adds an MVR membership group. <A.B.C.D> is the IP multicast group being added.

The count is the number of incremental multicast groups being added (the first multicast group is A.B.C.D). If a count is not specified, then only one multicast group is added.

**Format**

```
mvr group <A.B.C.D> [count]
```

**Mode**

- Global Config

**no mvr group**

This command removes the MVR membership group.

**Format**

```
no mvr group <A.B.C.D> [count]
```

**Mode**

- Global Config

**mvr mode**

This command changes the MVR mode type. If the mode is set to compatible, then the switch does not learn multicast groups; they need to be configured by the operator as the protocol does not forward joins from the hosts to the router. To operate in this mode, the IGMP router needs to be statically configured to transmit all required multicast streams to the MVR switch. If the mode is set to dynamic, then the switch learns existing multicast groups by snooping the IGMP queries from router on source ports and forwarding the IGMP joins from the hosts to the IGMP router on the multicast VLAN (with appropriate translation of the VLAN ID).

**Format**

```
mvr mode { compatible | dynamic }
```

**Mode**

- Global Config

**Default**

compatible
no mvr mode
This command sets the mode type to the default value.

Format  
Mode   

mvr querytime
This command sets the MVR query response time.

Format  mvr querytime <1-100>
Mode    Global Config
Default 5

no mvr querytime
This command sets the MVR query response time to the default value.

Format  no mvr querytime
Mode    Global Config

mvr vlan
This command sets the MVR multicast VLAN.

Format  mvr vlan <1-4094>
Mode    Global Config
Default 1

no mvr vlan
This command sets the MVR multicast VLAN to the default value.

Format  no mvr vlan
Mode    Global Config

mvr immediate
This command enables MVR immediate leave mode. MVR has two modes of operating with the IGMP Leave messages: normal leave and immediate leave:

- In normal leave mode, when a leave is received, the general IGMP query is sent from a Layer 2 switch to the receiver port, where the leave was received. Then reports are
Multicast VLAN Registration (MVR)

ProSafe Managed Switch

received from other interested hosts that are also connected to that port, for example, using hub.

- In immediate leave mode, when a leave is received, the switch is immediately reconfigured not to forward a specific multicast stream to the port where a message is received. This mode is used only for ports where only one client might be connected.

**Format**
mvr immediate

**Mode**
Interface Config

**Default**
Disabled

**no mvr immediate**

This command sets the MVR multicast VLAN to the default value.

**Format**
no mvr immediate

**Mode**
Interface Config

**mvr type**

This command sets the MVR port type. When a port is set as source, it is the port to which the multicast traffic flows using the multicast VLAN. When a port is set to receiver, it is the port where a listening host is connected to the switch.

**Format**
mvr type { receiver|source }

**Mode**
Interface Config

**Default**
one

**no mvr type**

Use this command to set the MVR port type to none.

**Format**
no mvr type

**Mode**
Interface Config

**mvr vlan group**

Use this command to include the port in the specific MVR group. <mVLAN> is the multicast VLAN, and <A.B.C.D> is the IP multicast group

**Format**
mvr vlan <mVLAN> group <A.B.C.D>

**Mode**
Interface Config
**no mvr vlan**

Use this command to exclude the port from the specific MVR group.

**Format**  
`no mvr vlan <mVLAN> group <A.B.C.D>`

**Mode**  
Interface Config

**show mvr**

This command displays global MVR settings.

**Format**  
`show mvr`

**Mode**  
Privileged EXEC

The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Running</td>
<td>MVR running state. It can be enabled or disabled.</td>
</tr>
<tr>
<td>MVR multicast VLAN</td>
<td>Current MVR multicast VLAN. It can be in the range from 1 to 4094.</td>
</tr>
<tr>
<td>MVR Max Multicast Groups</td>
<td>The maximum number of multicast groups supported by MVR.</td>
</tr>
<tr>
<td>MVR Current multicast groups</td>
<td>The current number of MVR groups allocated.</td>
</tr>
<tr>
<td>MVR Query response time</td>
<td>The current MVR query response time.</td>
</tr>
<tr>
<td>MVR Mode</td>
<td>The current MVR mode. It can be compatible or dynamic.</td>
</tr>
</tbody>
</table>

**Example:**

```
(Switch)#show mvr
MVR Running........................... TRUE
MVR multicast VLAN.................... 1200
MVR Max Multicast Groups.............. 256
MVR Current multicast groups......... 1
MVR Global query response time........ 10 (tenths of sec)
MVR Mode.............................. compatible
```

**show mvr members**

This command displays the MVR membership groups allocated. `<A.B.C.D>` is a valid multicast address in IPv4 dotted notation.

**Format**  
`show mvr members [<A.B.C.D>]`

**Mode**  
Privileged EXEC
The following table describes the output parameters.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR Group IP</td>
<td>MVR group multicast IP address.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the specific MVR group. It can be active or inactive.</td>
</tr>
<tr>
<td>Members</td>
<td>The list of ports that participates in the specified MVR group.</td>
</tr>
</tbody>
</table>

Example:

```
(switch)#show mvr members
MVR Group IP    Status   Members
------------------ --------------- ---------------------
224.1.1.1         INACTIVE      1/0/1, 1/0/2, 1/0/3

(switch)#show mvr members 224.1.1.1
MVR Group IP    Status   Members
------------------ --------------- ---------------------
224.1.1.1         INACTIVE      1/0/1, 1/0/2, 1/0/3
```

**show mvr interface**

This command displays the MVR-enabled interfaces configuration.

**Format**

```
show mvr interface [<interface-id> [members [vlan <vid>]]]
```

**Mode**

Privileged EXEC

The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Interface number</td>
</tr>
<tr>
<td>Type</td>
<td>The MVR port type. It can be none, receiver, or source type.</td>
</tr>
<tr>
<td>Status</td>
<td>The interface status. It consists of two characteristics:</td>
</tr>
<tr>
<td></td>
<td>• active or inactive indicates whether the port is forwarding.</td>
</tr>
<tr>
<td></td>
<td>• inVLAN or notInVLAN indicates whether the port is part of any VLAN.</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>The state of immediate mode. It can be enabled or disabled.</td>
</tr>
</tbody>
</table>

Example:

```
(switch)#show mvr interface
Port       Type       Status            Immediate Leave
---------- ------------ -------------- ------------------------
1/0/9       RECEIVER   ACTIVE/inVLAN   DISABLED
```
(switch)#show mvr interface 1/0/9
Type: RECEIVER Status: ACTIVE   Immediate Leave: DISABLED

(switch)#show mvr interface Fa1/0/23 members
235.0.0.1 STATIC   ACTIVE

(switch)#show mvr interface Fa1/0/23 members vlan 12
235.0.0.1 STATIC   ACTIVE
235.1.1.1 STATIC   ACTIVE

**show mvr traffic**

This command displays global MVR statistics.

**Format**

```
show mvr traffic
```

**Mode**

Privileged EXEC

The following table explains the output parameters.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Query Received</td>
<td>Number of received IGMP queries</td>
</tr>
<tr>
<td>IGMP Report V1 Received</td>
<td>Number of received IGMP reports V1</td>
</tr>
<tr>
<td>IGMP Report V2 Received</td>
<td>Number of received IGMP reports V2</td>
</tr>
<tr>
<td>IGMP Leave Received</td>
<td>Number of received IGMP leaves</td>
</tr>
<tr>
<td>IGMP Query Transmitted</td>
<td>Number of transmitted IGMP queries</td>
</tr>
<tr>
<td>IGMP Report V1 Transmitted</td>
<td>Number of transmitted IGMP reports V1</td>
</tr>
<tr>
<td>IGMP Report V2 Transmitted</td>
<td>Number of transmitted IGMP reports V2</td>
</tr>
<tr>
<td>IGMP Leave Transmitted</td>
<td>Number of transmitted IGMP leaves</td>
</tr>
<tr>
<td>IGMP Packet Receive Failures</td>
<td>Number of failures on receiving the IGMP packets</td>
</tr>
<tr>
<td>IGMP Packet Transmit Failures</td>
<td>Number of failures on transmitting the IGMP packets</td>
</tr>
</tbody>
</table>

**Example:**

(switch)#show mvr traffic

<table>
<thead>
<tr>
<th>IGMP Query Received...</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Report V1 Received...</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Report V2 Received...</td>
<td>3</td>
</tr>
<tr>
<td>IGMP Leave Received...</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Query Transmitted...</td>
<td>2</td>
</tr>
</tbody>
</table>
IGMP Report V1 Transmitted........................................... 0
IGMP Report V2 Transmitted........................................... 3
IGMP Leave Transmitted.................................................. 1
IGMP Packet Receive Failures........................................... 0
IGMP Packet Transmit Failures......................................... 0
This chapter describes the routing commands available in the 7000 series CLI.

**Note:** Commands described in this chapter that require a license are:
- *Router Discovery Protocol Commands*
- *Virtual Router Redundancy Protocol Commands*
- *Open Shortest Path First (OSPF) Commands*
- *OSPF Graceful Restart Commands*
- *Routing Information Protocol (RIP) Commands*

This chapter contains the following sections:

- *Address Resolution Protocol (ARP) Commands*
- *IP Routing Commands*
- *Router Discovery Protocol Commands*
- *Virtual LAN Routing Commands*
- *Virtual Router Redundancy Protocol Commands*
- *DHCP and BOOTP Relay Commands*
- *IP Helper Commands*
- *Open Shortest Path First (OSPF) Commands*
- *OSPF Graceful Restart Commands*
- *Routing Information Protocol (RIP) Commands*
- *ICMP Throttling Commands*

The commands in this chapter are in 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.
**Address Resolution Protocol (ARP) Commands**

This section describes the commands you use to configure 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.

**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. `<macaddr>` is a unicast MAC address for that device.

The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

**Format**

```
arp <ipaddress> <macaddr>
```

**Mode**

Global Config

**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. `<macaddr>` is a unicast MAC address for that device.

**Format**

```
no arp <ipaddress> <macaddr>
```

**Mode**

Global Config

**ip proxy-arp**

This command enables proxy ARP on a router interface. 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

**no ip proxy-arp**

This command disables proxy ARP on a router interface.

**Format**

```
no ip proxy-arp
```

**Mode**

Interface Config
**arp cachesize**

This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

**Format**

```
arp cachesize <platform specific integer value>
```

**Mode**

Global Config

**no arp cachesize**

This command configures the default ARP cache size.

**Format**

```
no arp cachesize
```

**Mode**

Global Config

**arp dynamicrenew**

This command enables the ARP component to automatically renew dynamic ARP entries when they age out.

**Default**

enabled

**Format**

```
arp dynamicrenew
```

**Mode**

Privileged EXEC

**no arp dynamicrenew**

This command prevents dynamic ARP entries from renewing when they age out.

**Format**

```
no arp dynamicrenew
```

**Mode**

Privileged EXEC

**arp purge**

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

**Format**

```
arp purge <ipaddr>
```

**Mode**

Privileged EXEC

**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

**no arp resptime**

This command configures the default ARP request response timeout.

**Format** `no arp resptime`

**Mode** Global Config

**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

**no arp retries**

This command configures the default ARP count of maximum request for retries.

**Format** `no arp retries`

**Mode** Global Config

**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
no arp timeout

This command configures the default ARP entry ageout time.

Format:     no arp timeout
Mode:       Global Config

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

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

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>
</tbody>
</table>
The following are displayed for each ARP entry:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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 Configured/Active / Max</td>
<td>The static entry count in the ARP table, the active entry count in the ARP table, the active entry count in the ARP table, and maximum static entry count in the ARP table.</td>
</tr>
</tbody>
</table>

show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format: show arp brief

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 value 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>
show arp switch

This command displays the contents of the switch’s Address Resolution Protocol (ARP) table.

Format:  `show arp switch`
Mode:    Privileged EXEC

<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 the switch.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The hardware MAC address of that device.</td>
</tr>
<tr>
<td>Interface</td>
<td>The routing unit/slot/port associated with the device’s ARP entry.</td>
</tr>
</tbody>
</table>

IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

routing

This command enables IPv4 and IPv6 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.”

Default:       disabled
Format:        routing
Mode:          Interface Config

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

ip routing

This command enables the IP Router Admin Mode for the master switch.

Format:       ip routing
Mode:         Global Config
no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format: no ip routing
Mode: Global Config

ip address

This command configures an IP address on an interface. You can also use this command to configure one or more secondary IP addresses on the interface. The value for `<ipaddr>` is the IP address of the interface. The value for `<subnetmask>` is a 4-digit dotted-decimal number which represents the subnet mask of the interface. The subnet mask must have contiguous ones and be no longer than 30 bits, for example 255.255.255.0. This command adds the label IP address in `show ip interface`.

Format: ip address <ipaddr> <subnetmask> [secondary]
Mode: Interface Config

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

ip address dhcp

Use this command to enable 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.

Default: disabled
Format: ip address dhcp
Mode: Interface Config
no ip address dhcp

Use this command to release a leased address and disable DHCPv4 on an interface.

Format: `no ip address dhcp`
Mode: Interface Config

ip default-gateway

Use this command to manually configure a default gateway for the switch. Only one default gateway can be configured. If you use this command multiple times, each command replaces the previous value.

Format: `ip default-gateway <ipaddr>`
Mode: Global Config

no ip default-gateway

Use this command to remove the default gateway address from the configuration.

Format: `no ip default-gateway <ipaddr>`
Mode: Interface Config

release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface.

Format: `release dhcp <unit/slot/port>`
Mode: Privileged EXEC

renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

Format: `renew dhcp {<unit/slot/port>|network-port}`
Mode: Privileged EXEC

**Note:** This command can be used on in-band ports as well as network (out-of-band) port.
**show dhcp lease**

Use this command to display 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 <unit/slot/port>]
```

**Mode**

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>

**ip route**

This command configures a static route. The `<ipaddr>` parameter is a valid IP address, and `<subnetmask>` is a valid subnet mask. The `<nexthopip>` parameter is a valid IP address of the next hop router. Specifying Null0 as nexthop parameter adds a static reject route. The optional `<preference>` parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
• Confirm that the associated link is also up.

**Default** preference—1

**Format** `ip route <ipaddr> <subnetmask> [nexthopip | Null0] [preference]`

**Mode** Global Config

**no ip route**

This command deletes a single next hop to a destination static route. If you use the `nexthopip` parameter, the next hop is deleted. If you use the `preference` value, the preference value of the static route is reset to its default.

**Format** `no ip route <ipaddr> <subnetmask> [nexthopip | Null0] [preference]`

**Mode** Global Config

**ip route default**

This command configures the default route. The value for `nexthopip` is a valid IP address of the next hop router. The `preference` is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

**Default** preference—1

**Format** `ip route default nexthopip [preference]`

**Mode** Global Config

**no ip route default**

This command deletes all configured default routes. If the optional `nexthopip` parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

**Format** `no ip route default [nexthopip | preference]`

**Mode** Global Config

**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

**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

**ip netdirbcast**

This command enables the forwarding of network-directed broadcasts. When enabled,
network directed broadcasts are forwarded. When disabled they are dropped.

Default: disabled
Format: ip netdirbcast
Mode: Interface Config

**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

**ip mtu**

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface. The IP
MTU is the size of the largest IP packet that can be transmitted on the interface without
fragmentation. The software currently does not fragment IP packets.

- Packets forwarded in hardware ignore the IP MTU.
- Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing
  interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.
The IP stack uses its default IP MTU and ignores the value set using the `ip mtu` command.
OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the `ip ospf mtu-ignore` command.)

**Note:** The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see `mtu` on page 40) must take into account the size of the Ethernet header.

### Default
1500 bytes

### Format
`ip mtu <68-9198>`

### Mode
Interface Config

**no ip mtu**

This command resets the ip mtu to the default value.

### Format
`no ip mtu <mtu>`

### Mode
Interface Config

**encapsulation**

This command configures the link layer encapsulation type for the packet. The encapsulation type can be `ethernet` or `snap`.

### Default
ethernet

### Format
`encapsulation {ethernet | snap}`

### Mode
Interface Config

**Note:** Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.
clear ip route all

This command removes all the route entries learned over the network.

Format: clear ip route all
Mode: Privileged EXEC
Protocol: Tells which protocol added the specified route. The possibilities are: local, static, OSPF, or RIP.
Total Number of Routes: The total number of routes.

show ip brief

This command displays all the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.

Format: show ip brief
Modes: Privileged EXEC, User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Time to Live</td>
<td>The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.</td>
</tr>
<tr>
<td>Routing Mode</td>
<td>Shows whether the routing mode is enabled or disabled.</td>
</tr>
<tr>
<td>Maximum Next Hops</td>
<td>The maximum number of next hops the packet can travel.</td>
</tr>
<tr>
<td>Maximum Routes</td>
<td>The maximum number of routes the packet can travel.</td>
</tr>
</tbody>
</table>
| ICMP Rate Limit Burst Interval    | Shows how often the token bucket is initialized with burst-size tokens. 
Burst-interval is from 0 to 2147483647 milliseconds. The default burst-interval is 1000 msec. |
| ICMP Rate Limit Burst Size       | Shows the number of ICMPv4 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages. The default value is 100 messages. |
| ICMP Echo Replies                 | Shows whether ICMP Echo Replies are enabled or disabled.                  |
| ICMP Redirects                   | Shows whether ICMP Redirects are enabled or disabled.                     |

The following shows example CLI display output for the command.

(Switch) #show ip brief

Default Time to Live......................... 64
Routing Mode.................................... Disabled
Maximum Next Hops............................ 4
Maximum Routes................................ 6000
ICMP Rate Limit Interval....................... 1000 msec
ICMP Rate Limit Burst Size..................... 100 messages
ICMP Echo Replies.............................. Enabled
ICMP Redirects................................. Enabled

**show ip interface**

This command displays all pertinent information about the IP interface.

**Format**

show ip interface {<unit/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>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 ip helper-address (Global Config) command.</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>
<tr>
<td>Local Proxy ARP</td>
<td>Displays whether Local Proxy ARP is enabled or disabled on the interface.</td>
</tr>
<tr>
<td>Active State</td>
<td>Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.</td>
</tr>
<tr>
<td>Link Speed Data Rate</td>
<td>An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.</td>
</tr>
<tr>
<td>Encapsulation Type</td>
<td>The encapsulation type for the specified interface. The types are: Ethernet or SNAP.</td>
</tr>
<tr>
<td>IP MTU</td>
<td>The maximum transmission unit (MTU) size of a frame, in bytes.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Shows the bandwidth of the interface.</td>
</tr>
</tbody>
</table>
Routing Commands

ProSafe Managed Switch

The following shows example CLI display output for the command.

(switch)#show ip interface 1/0/2

Routing Interface Status....................... Down
Primary IP Address................................ 1.2.3.4/255.255.255.0
Secondary IP Address(es)........................... 21.2.3.4/255.255.255.0
............................................... 22.2.3.4/255.255.255.0
Helper IP Address.............................. 1.2.3.4
............................................... 1.2.3.5
Routing Mode................................... Disable
Administrative Mode............................ Enable
Forward Net Directed Broadcasts................ Disable
Proxy ARP...................................... Enable
Local Proxy ARP................................ Disable
Active State................................... Inactive
Link Speed Data Rate........................... Inactive
MAC Address.................................... 00:10:18:82:0C:68
Encapsulation Type............................. Ethernet
IP MTU......................................... 1500
Bandwidth...................................... 100000 kbps
Destination Unreachables....................... Enabled
ICMP Redirects.................................. Enabled

show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

Format: show ip interface brief
Modes:
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Unreachables</td>
<td>Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).</td>
</tr>
<tr>
<td>ICMP Redirects</td>
<td>Displays whether ICMP Redirects may be sent (enabled or disabled).</td>
</tr>
</tbody>
</table>
**Routing Commands**

**ProSafe Managed Switch**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netdir Bcast</td>
<td>Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.</td>
</tr>
<tr>
<td>MultiCast Fwd</td>
<td>The multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.</td>
</tr>
</tbody>
</table>

**show ip route**

This command displays the routing table. The `<ip-address>` specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The `<mask>` specifies the subnet mask for the given `<ip-address>`. When you use the `longer-prefixes` keyword, the `<ip-address>` and `<mask>` pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the `<protocol>` parameter to specify the protocol that installed the routes. The value for `<protocol>` can be `connected`, `ospf`, `rip`, or `static`. Use the all parameter to display all routes including best and non-best routes. If you do not use the all parameter, the command only displays the best route.

*Note:* If you use the `connected` keyword for `<protocol>`, the all option is not available because there are no best or non-best connected routes.

**Format**

```
show ip route [{<ip-address> [<protocol>] | {<ip-address> <mask> [longer-prefixes] [<protocol>]} | <protocol> [all] | all}]
```

**Modes**

- Privileged EXEC
- User EXEC

<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:

```
Code IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface
```

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 codes for the routing protocols that created the routes.</td>
</tr>
<tr>
<td>IP-Address/Mask</td>
<td>The IP-Address and mask of the destination network corresponding to this route.</td>
</tr>
<tr>
<td>Preference</td>
<td>The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.</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.

The following shows example CLI display output for the command.

```plaintext
(Switch) #show ip route
```

```
Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
B - BGP Derived, IA - OSPF Inter Area
E1 - OSPF External Type 1, E2 - OSPF External Type 2
N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2, 00h:00m:01s, 0/5
C 11.11.11.0/24 [0/1] directly connected, 0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
```

**show ip route summary**

Use this command to display the routing table summary. Use the optional **all** parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

**Format**

```
show ip route summary [all]
```

**Modes**

- Privileged EXEC
- User EXEC

---

**Routing Commands**

248
The following shows example CLI display output for the command.

(Switch) #show ip route summary

Connected Routes..............................1
Static Routes.................................7
RIP Routes....................................0
BGP Routes....................................0
OSPF Routes...................................0
   Intra Area Routes.........................0
   Inter Area Routes........................0
   External Type-1 Routes....................0
   External Type-2 Routes....................0
Reject Routes.................................2
Total routes..................................8

show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format  show ip route preferences
Modes   • Privileged EXEC
          • User EXEC

<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>
</tbody>
</table>
**show ip stats**

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

**Format**

show ip stats

**Modes**

- Privileged EXEC
- User EXEC

**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.

**ip irdp**

This command enables Router Discovery on an interface.

**Default**

disabled

**Format**

ip irdp

**Mode**

Interface Config

**no ip irdp**

This command disables Router Discovery on an interface.

**Format**

no ip irdp

**Mode**

Interface Config

**ip irdp multicast**

This command configures the address that the interface uses to send the router discovery advertisements. The address is 224.0.0.1, which is the all-hosts IP multicast address.

**Default**

224.0.0.1

**Format**

ip irdp multicast

**Mode**

Interface Config
no ip irdp multicast

This command configures the address used to advertise the router to the Broadcast address (255.255.255.155).

Format: no ip irdp multicast
Mode: Interface Config

ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of <maxadvertinterval> to 9000 seconds.

Default: 3 * maxinterval
Format: ip irdp holdtime <maxadvertinterval-9000>
Mode: Interface Config

no ip irdp holdtime

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Format: no ip irdp holdtime
Mode: Interface Config

ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for maxadvertinterval is 4 to 1800 seconds.

Default: 600
Format: ip irdp maxadvertinterval <4-1800>
Mode: Interface Config

no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format: no ip irdp maxadvertinterval
Mode: Interface Config
**ip irdp minadvertinterval**

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is three to the value of maxadvertinterval.

**Default**

<table>
<thead>
<tr>
<th>Format</th>
<th>ip irdp minadvertinterval &lt;3-maxadvertinterval&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**no ip irdp minadvertinterval**

This command sets the default minimum time to the default.

**Format**

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip irdp minadvertinterval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Format</th>
<th>ip irdp preference &lt;-2147483648 to 2147483647&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**no ip irdp preference**

This command configure the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

**Format**

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip irdp preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**show ip irdp**

This command displays the router discovery information for all interfaces, or a specified interface.

**Format**

| Format | show ip irdp {<unit/slot/port> | all} |
|--------|-----------------------------------|
| Modes  | Privileged EXEC                   |
|        | User EXEC                          |
Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

**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 that is already in use, the CLI displays an error message and does not create the VLAN interface.

**Format**

```
vlan routing <vlanid> [interface ID]
```

**Mode**

VLAN Config

**no vlan routing**

This command deletes routing on a VLAN. The `<vlanid>` value has a range from 1 to 4093.

**Format**

```
no vlan routing <vlanid>
```

**Mode**

VLAN Config

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The <code>&lt;unit/slot/port&gt;</code> that matches the rest of the information in the row.</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>Advertise Address</td>
<td>The IP address to which the interface sends the advertisement.</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>
**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</td>
<td>The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.</td>
</tr>
<tr>
<td>Routing VLANs</td>
<td>The identifier of the VLAN.</td>
</tr>
<tr>
<td>Logical Interface</td>
<td>The logical unit/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>

**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.

**ip vrrp (Global Config)**

Use this command in Global Config mode to enable the administrative mode of VRRP on the router.

**Default**

`none`

**Format**

`ip vrrp`

**Mode**

Global Config

**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
**ip vrrp (Interface Config)**

Use this command in Interface Config mode to create a virtual router associated with the interface. 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

**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**

```
o ip vrrp <vrid>
```

**Mode**

Interface Config

**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

**no ip vrrp mode**

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

**Format**

```
o ip vrrp <vrid> mode
```

**Mode**

Interface Config

**ip vrrp ip**

This command sets the virtual router IP address value for an interface. 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
Routing Commands

ProSafe Managed Switch

Format: ip vrrp <vrid> ip <ipaddr> [secondary]
Mode: Interface Config

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

ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface. 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

no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface.

Format: no ip vrrp <vrid> authentication
Mode: Interface Config

ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface. 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
no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface.

Format no ip vrrp <vrid> preempt
Mode Interface Config

ip vrrp priority

This command sets the priority of a router within a VRRP group. Higher values equal higher priority. The range is from 1 to 254. The parameter <vrid> is the virtual router ID, whose range is from 1 to 255.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the “address owner.” The priority of the address owner is always 255 so that the address owner is always master. If the master has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the master’s priority, the router will take over as master only if preempt mode is enabled.

Default 100 unless the router is the address owner, in which case its priority is automatically set to 255.

Format ip vrrp <vrid> priority <1-254>
Mode Interface Config

no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface.

Format no ip vrrp <vrid> priority
Mode Interface Config

ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface on the specified virtual router sends a virtual router advertisement.

Default 1

Format ip vrrp <vrid> timers advertise <1-255>
Mode Interface Config
no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface.

Format  no ip vrrp <vrid> timers advertise
Mode     Interface Config

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.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the <priority> argument. When the interface is up for IP protocol, the priority will be incremented by the <priority> value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, the priority of the router will be decreased by 10 (the default priority decrement) for each downed interface. The default priority decrement is changed using the <priority> argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10.

Default  priority: 10
Format     ip vrrp <vrid> track interface <unit/slot/port> [decrement <priority>]
Mode       Interface Config

no ip vrrp track interface

Use this command to remove the interface from the tracked list or to restore the priority decrement to its default.

Format     no ip vrrp <vrid> track interface <unit/slot/port> [decrement]
Mode       Interface Config

ip vrrp track ip route

Use this command to track the route reachability. 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)
Routing Commands

ProSafe Managed Switch

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

Format

Mode

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

Mode

ip vrrp <vrid> accept-mode

This command is used to allow a router to respond to ICMP Echo Requests sent to an address on a VRRP virtual router. VRRP supports responding to pings, but does not allow the VRRP Master to accept other types of packets. A new configuration option controls whether the router responds to Echo Requests sent to a VRRP IP address.

The VRRP Master responds to both fragmented and un-fragmented ICMP Echo Request packets. The VRRP Master responds to Echo Requests sent to the virtual router's primary address or any of its secondary addresses.

Ping to a VRRP IP address only works from the host side (where the VRRP router is configured). There is no value in pinging to the VRRP IP from another interface because packet flow from the network to the host doesn't involve VRRP. This is used only to troubleshoot a connectivity problem for traffic originating on the VRRP protected LAN.

Members of the virtual router who are in backup state discard ping packets destined to VRRP address(es), just as they discard any Ethernet frame sent to a VRRP MAC address. When the VRRP master responds with an Echo Reply, the source IPv4 address is the VRRP address and source MAC address is the virtual router's MAC address.

There is a separate command "ip icmp echo-reply" that controls whether the router responds to ICMP Echo Requests. When Echo Replies are disabled using that command, the VRRP master does not respond to Echo Requests, even if this new option is enabled.

Default

Format

Mode
**no ip vrrp vrid accept-mode**

This command is used to allow a router to respond to ICMP Echo Requests sent to an address on a VRRP virtual router.

**Format**

no ip vrrp <vrid> accept-mode

**Mode**

Interface Config

**show ip vrrp interface stats**

This command displays the statistical information about each virtual router configured on the switch.

**Format**

show ip vrrp interface stats <unit/slot/port> <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>
<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 PacketsReceived</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>
</tbody>
</table>
### Routing Commands

**show ip vrrp**

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring. This command takes no options.

**Format**

```
show ip vrrp
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>

**show ip vrrp interface**

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface. Use the output of the command to verify the track interface and track IP route configurations.

**Format**

```
show ip vrrp interface {<interface-name> <vrid> }
```

**Modes**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary IP Address</td>
<td>The configured IP address for the Virtual router.</td>
</tr>
<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>
</tbody>
</table>
Routing Commands

ProSafe Managed Switch

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured Priority</td>
<td>The priority configured through the <strong>ip vrrp</strong> <code>&lt;vr&gt; priority &lt;1-254&gt;</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>State</td>
<td>The state (Master/backup) of the virtual router.</td>
</tr>
</tbody>
</table>

The following shows example CLI display output for the command.

(Switch)#show ip vrrp interface 1/0/1 1

Primary IP Address............................. 1.1.1.5
VMAC Address................................... 00:00:5e:00:01:01
Authentication Type............................ None
Priority....................................... 100
    Configured priority......................... 100
Advertisement Interval (secs)................. 1
Pre-empt Mode.................................. Enable
Administrative Mode............................ Disable
Accept Mode.................................... Enable
State.......................................... Initialized

<table>
<thead>
<tr>
<th>Track Interface</th>
<th>State</th>
<th>DecrementPriority</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1/0/1&gt;</td>
<td>down</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TrackRoute  (pfx/len)</th>
<th>State</th>
<th>DecrementPriority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1/255.255.255.0</td>
<td>down</td>
<td>10</td>
</tr>
</tbody>
</table>

**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>Valid slot and port number separated by forward slashes.</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>
</tbody>
</table>
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.

**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

**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

**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

**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
**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

**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

**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>Server IP Address</td>
<td>The IP address for the BootP/DHCP Relay server.</td>
</tr>
<tr>
<td>Circuit Id Option Mode</td>
<td>The DHCP circuit Id option which may be enabled or disabled.</td>
</tr>
<tr>
<td>Requests Received</td>
<td>The number or requests received.</td>
</tr>
<tr>
<td>Requests Relayed</td>
<td>The number of requests relayed.</td>
</tr>
<tr>
<td>Packets Discarded</td>
<td>The number of packets discarded.</td>
</tr>
</tbody>
</table>
IP Helper Commands

This section describes the commands to configure a DHCP relay agent with multiple DHCP server addresses per routing interface, and to use different server addresses for client packets arriving on different interfaces on the relay agent.

clear ip helper statistics

Use this command to reset the statistics displayed in the show ip helper statistics command to zero.

Format  clear ip helper statistics
Mode    Privileged EXEC

ip helper-address (Global Config)

Use the Global Configuration ip helper-address command to have the switch forward User Datagram Protocol (UDP) broadcasts received on an interface. To disable the forwarding of broadcast packets to specific addresses, use the no form of this command.

The ip helper-address command forwards specific UDP broadcast from one interface to another. You can define many helper addresses but the total number of address-port pairs is limited to 128 for the whole device. The setting of a helper address for a specific interface has precedence over a setting of a helper address for all interfaces.

Ip-address: Destination broadcast or host address to be used when forwarding UDP broadcasts. You can specify 0.0.0.0 to indicate not to forward the UDP packet to any host and use "255.255.255.255" to broadcast the UDP packets to all hosts on the target subnet.

udp-port-list: The broadcast packet destination UDP port number to forward. If not specified, packets for the default services are forwarded to the helper address. Valid range, 0-65535.

Default     Disabled
Format       ip helper-address <ip-address>
             {<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|
             netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}
Mode         Global Config

no ip helper-address (Global Config)

Use this command to remove the IP address from the previously configured list. The no command without an <ip-address> argument removes the entire list of helper addresses on that interface.

Format      no ip helper-address {<ip-address>}
             {<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|
             netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}
Mode        Global Config
**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

**no ip helper enable**

Use this command to disable relay of all UDP packets.

- **Format:** `no ip helper enable`
- **Mode:** Global Config

**ip helper-address**

Use this command to add a unicast helper address to the list of helper addresses on an interface. This is the address of a DHCP server. This command can be applied multiple times on the routing interface to form the helper addresses list until the list reaches the maximum supported helper addresses.

- **Format:** `ip helper-address <ip-address>
  [dhcp|domain|isakmp|mobile-ip|nameserver|
  netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time]`
- **Mode:** Interface Config

**no ip helper-address**

Use this command to remove the IP address from the previously configured list. The no command without an `<ip-address>` argument removes the entire list of helper addresses on that interface.

- **Format:** `no ip helper-address {<ip-address>}
  [dhcp|domain|isakmp|mobile-ip|nameserver|
  netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time]`
- **Mode:** Interface Config
**ip helper-address discard**

Use this command to drop matching packets.

Format:

```
ip helper-address discard
{<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|
etbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}
```

Mode: Interface Config

**no ip helper-address discard**

Use this command to permit the matching packets.

Format:

```
o ip helper-address discard
{<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|
etbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}
```

Mode: Interface Config

**show ip helper-address**

Use this command to display the configured helper addresses on the given interface.

Format:

```
show ip helper-address <interface>
```

Mode:
- Privileged EXEC
- User EXEC

The following shows example CLI display output for the command.

```
(switch) #show ip helper-address 1/0/1
Helper IP Address.............................. 1.2.3.4
............................................... 1.2.3.5
```

**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>Term</th>
<th>Definition</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 incremented only 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&gt;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>
</tbody>
</table>
Open Shortest Path First (OSPF) Commands

This section describes the commands you use to view and configure OSPF, which is a link-state routing protocol that you use to route traffic within a network.

**router ospf**

Use this command to enter Router OSPF mode.

<table>
<thead>
<tr>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>router ospf</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server messages received</td>
<td>The number of DHCP responses received from the DHCP server. This count includes only 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>
### enable (OSPF)

This command resets the default administrative mode of OSPF in the router (active).

<table>
<thead>
<tr>
<th>Default</th>
<th>enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>enable</td>
</tr>
<tr>
<td>Mode</td>
<td>Router OSPF Config</td>
</tr>
</tbody>
</table>

### no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

<table>
<thead>
<tr>
<th>Format</th>
<th>no enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Router OSPF Config</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>network &lt;ip-address&gt; &lt;wildcard-mask&gt; area &lt;area-id&gt;</td>
</tr>
<tr>
<td>Mode</td>
<td>Router OSPF Config</td>
</tr>
</tbody>
</table>

### no network area (OSPF)

Use this command to disable the OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command.

<table>
<thead>
<tr>
<th>Format</th>
<th>no network &lt;ip-address&gt; &lt;wildcard-mask&gt; area &lt;area-id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Router OSPF Config</td>
</tr>
</tbody>
</table>

### ip ospf area

Use this command to enable OSPFv2 and set the area ID of an interface. 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.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip ospf area &lt;area-id&gt; [secondaries none]</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>
no ip ospf area

Use this command to disable OSPF on an interface.

Format: no ip ospf area [secondaries none]
Mode: Interface Config

1583compatibility

This command enables OSPF 1583 compatibility.

Note: 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Default: enabled
Format: 1583compatibility
Mode: Router OSPF Config

no 1583compatibility

This command disables OSPF 1583 compatibility.

Format: no 1583compatibility
Mode: Router OSPF Config

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

area nssa (OSPF)

This command configures the specified areaid to function as an NSSA.

Format: area <areaid> nssa
Mode: Router OSPF Config
no area nssa

This command disables nssa from the specified area id.

**Format**

```
no area <areaid> nssa
```

**Mode**

Router OSPF Config

---

**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 10. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

**Format**

```
area <areaid> nssa default-info-originate [<metric>] [{comparable | non-comparable}]
```

**Mode**

Router OSPF Config

---

**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

---

**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

---

**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
**area nssa no-summary (OSPF)**

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

*Format*  
```text
area <areaid> nssa no-summary
```

*Mode*  
Router OSPF Config

**no area nssa no-summary (OSPF)**

This command disables nssa from the summary LSAs.

*Format*  
```text
no area <areaid> nssa no-summary
```

*Mode*  
Router OSPF Config

**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*  
```text
area <areaid> nssa translator-role {always | candidate}
```

*Mode*  
Router OSPF Config

**no area nssa translator-role (OSPF)**

This command disables the nssa translator role from the specified area id.

*Format*  
```text
no area <areaid> nssa translator-role {always | candidate}
```

*Mode*  
Router OSPF Config

**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*  
```text
area <areaid> nssa translator-stab-intv <stabilityinterval>
```

*Mode*  
Router OSPF Config
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`

area range (OSPF)

This command creates a specified area range for a specified NSSA. The <ipaddr> is a valid IP address. The <subnetmask> is a valid subnet mask. The LSDB type must be specified by either `summarylink` or `nssaexternallink`, and the advertising of the area range can be allowed or suppressed.

Format: `area <areaid> range <ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise | not-advertise]

Mode: `Router OSPF Config`

no area range

This command deletes a specified area range. The <ipaddr> is a valid IP address. The <subnetmask> is a valid subnet mask.

Format: `no area <areaid> range <ipaddr> <subnetmask>

Mode: `Router OSPF Config`

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`

no area stub

This command deletes a stub area for the specified area ID.

Format: `no area <areaid> stub`

Mode: `Router OSPF Config`
area stub no-summary (OSPF)

This command configures the Summary LSA mode for the stub area identified by \(<\text{areaid}>\). Use this command to prevent LSA Summaries from being sent.

Default: disabled

Format: `area <areaid> stub no-summary`

Mode: Router OSPF Config

no area stub no-summary

This command configures the default Summary LSA mode for the stub area identified by \(<\text{areaid}>\).

Format: `no area <areaid> stub no-summary`

Mode: Router OSPF Config

area virtual-link (OSPF)

This command creates the OSPF virtual interface for the specified \(<\text{areaid}>\) and \(<\text{neighbor}>\). The \(<\text{neighbor}>\) parameter is the Router ID of the neighbor.

Format: `area <areaid> virtual-link <neighbor>`

Mode: Router OSPF Config

no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by \(<\text{areaid}>\) and \(<\text{neighbor}>\). The \(<\text{neighbor}>\) parameter is the Router ID of the neighbor.

Format: `no area <areaid> virtual-link <neighbor>`

Mode: Router OSPF Config

area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by \(<\text{areaid}>\) and \(<\text{neighbor}>\). The \(<\text{neighbor}>\) parameter is the Router ID of the neighbor. The value for \(<\text{type}>\) is either none, simple, or encrypt. The \([\text{key}]\) is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id in the range of 0 and 255 must be
specified. The default value for authentication type is none. Neither the default password key nor the default key id are configured.

Default

Format

Mode

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

Mode

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

Format

Mode

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

Mode

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

Format

Mode
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

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

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

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

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
**auto-cost (OSPF)**

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the `auto-cost reference-bandwidth` and `bandwidth` commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where interface bandwidth is defined by the `bandwidth` command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the `auto-cost` command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1-4294967 Mbps. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

**Default**

100Mbps

**Format**

`auto-cost reference-bandwidth <1 to 4294967>`

**Mode**

Router OSPF Config

---

**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

---

**bandwidth**

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the `auto-cost` command. For the purpose of the OSPF link cost calculation, use the `bandwidth` command to specify the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface.

**Default**

actual interface bandwidth

**Format**

`bandwidth <1-1000000>`

**Mode**

Interface Config
no bandwidth

Use this command to set the interface bandwidth to its default value.

Format  
no bandwidth
Mode  
Interface Config

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. The 7000 series supports the storing and flooding of Opaque LSAs of different scopes.

Default  
disabled
Format  
capability opaque
Mode  
Router OSPF Config

no capability opaque

Use this command to disable opaque capability on the router.

Format  
no capability opaque
Mode  
Router OSPF Config

clear ip ospf

Use this command to disable and re-enable OSPF.

Format  
clear ip ospf
Mode  
Privileged EXEC

clear ip ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format  
clear ip ospf configuration
Mode  
Privileged EXEC

clear ip ospf counters

Use this command to reset global and interface statistics.

Format  
clear ip ospf counters
Mode  
Privileged EXEC
**clear ip ospf neighbor**

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor’s interface, send a one-way hello. Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor’s Router ID using the optional parameter [neighbor-id].

**Format**

`clear ip ospf neighbor [neighbor-id]`

**Mode**

Privileged EXEC

**clear ip ospf neighbor interface**

To drop adjacency with all neighbors on a specific interface, use the optional parameter [unit/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 [unit/slot/port] [neighbor-id]`

**Mode**

Privileged EXEC

**clear ip ospf redistribution**

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

**Format**

`clear ip ospf redistribution`

**Mode**

Privileged EXEC

**clear ip ospf stub-router**

OSPF can enter stub router mode due to resource exhaustion (too many LSA’s, too many routes, memory allocation failures etc). When this happens, the user can get out of this mode by issuing the command after the cause of the overload has been resolved.

**Format**

`clear ip ospf stub-router`

**Mode**

Privileged EXEC

**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
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

**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

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

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

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
**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

**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

**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

**no exit-overflow-interval**

This command configures the default exit overflow interval for OSPF.

**Format**
no exit-overflow-interval

**Mode**
Router OSPF Config

**external-lsdb-limit (OSPF)**

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for limit is -1 to 2147483647.

**Default**
-1

**Format**
external-lsdb-limit <limit>

**Mode**
Router OSPF Config
no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format  no external-lsdb-limit
Mode    Router OSPF Config

ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface. The value of <type> is either none, simple or encrypt. The <key> is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. If the type is encrypt a <keyid> in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID. There is no default value for this command.

Format  ip ospf authentication {none | {simple <key>} | {encrypt <key> <keyid>}}
Mode    Interface Config

no ip ospf authentication

This command sets the default OSPF Authentication Type for the specified interface.

Format  no ip ospf authentication
Mode    Interface Config

ip ospf cost

This command configures the cost on an OSPF interface. The <cost> parameter has a range of 1 to 65535.

Default  10
Format    ip ospf cost <1-65535>
Mode      Interface Config

no ip ospf cost

This command configures the default cost on an OSPF interface.

Format  no ip ospf cost
Mode    Interface Config
**ip ospf dead-interval**

This command sets the OSPF dead interval for the specified interface. The value for `<seconds>` is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range in seconds from 1 to 2147483647.

```
Default: 40
Format:   ip ospf dead-interval <seconds>
Mode:     Interface Config
```

**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
```

**ip 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 range from 1 to 65535.

```
Default: 10
Format:   ip ospf hello-interval <seconds>
Mode:     Interface Config
```

**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
```

**ip ospf network**

Use this command to configure OSPF to treat an interface 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

**no ip ospf network**

Use this command to return the OSPF network type to the default.

Format: no ip ospf network

Mode: Interface Config

**ip ospf priority**

This command sets the OSPF priority for the specified router interface. The priority of the interface is an 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

**no ip ospf priority**

This command sets the default OSPF priority for the specified router interface.

Format: no ip ospf priority

Mode: Interface Config

**ip ospf retransmit-interval**

This command sets the OSPF retransmit interval for the specified interface. 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
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

ip ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. 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

no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format  
no ip ospf transmit-delay

Mode  
Interface Config

ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default  
enabled

Format  
ip ospf mtu-ignore

Mode  
Interface Config

no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format  
no ip ospf mtu-ignore

Mode  
Interface Config
**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

**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

**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

**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

**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
**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

**no passive-interface default**

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Format: `no passive-interface default`

Mode: Router OSPF Config

**passive-interface (OSPF)**

Use this command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Default: disabled

Format: `passive-interface {<unit/slot/port>}`

Mode: Router OSPF Config

**no passive-interface**

Use this command to set the interface or tunnel as non-passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Format: `no passive-interface {<unit/slot/port>}`

Mode: Router OSPF Config

**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
**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 1**.

**Table 1. Trapflags Groups**

<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>if-rx</td>
<td>ir-rx-packet</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>rtb</td>
<td>• rtb-entry-info</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**.
no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the `group name` followed by that particular flag.
- To disable all the flags in that group, give the group name followed by `all`.
- To disable all the flags, give the command as `trapflags all`.

```
Format

no trapflags {
  all |
  errors {all | authentication-failure | bad-packet | config-error |
  virt-
  authentication-failure | virt-bad-packet | virt-config-error} |
  if-rx {all | if-rx-packet} |
  lsa {all | lsa-maxage | lsa-originate} |
  overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
  retransmit {all | packets | virt-packets} |
  rtb {all, rtb-entry-info} |
  state-change {all | if-state-change | neighbor-state-change |
  virtif-state-
  change | virtneighbor-state-change}
}
```

Mode Router OSPF Config
**show ip ospf**

This command displays information relevant to the OSPF router.

**Format**

```
show ip ospf
```

**Mode**

Privileged EXEC

---

**Note:** Some of the information below displays only if you enable OSPF and configure certain features.

<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>ASBR Mode</td>
<td>Indicates whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocols. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).</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 non-default 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>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>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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stub Router</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 re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.</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>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 LSAChecksum</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 AS Opaque 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>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>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>Default Metric</td>
<td>Default value for redistributed routes.</td>
</tr>
<tr>
<td>Default Passive Setting</td>
<td>Shows whether the interfaces are passive by default.</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>
</tbody>
</table>
The following shows example CLI display output for the command.

(Switch) #show ip ospf

Router ID.................................2.2.2.2
OSPF Admin Mode.........................Disable
RFC 1583 Compatibility..................Enable
External LSDB Limit......................No Limit
Exit Overflow Interval..................0
Spf Delay Time..........................5
Spf Hold Time...........................10
Opaque Capability.......................Disable
AutoCost Ref BW..........................100 Mbps
Default Passive Setting.................Disabled
Maximum Paths...........................4
Default Metric...........................Not configured

Default Route Advertise.................Disabled
Always....................................FALSE
Metric...................................Not configured
Metric Type..............................External Type 2

Number of Active Areas...................3 (3 normal, 0 stub, 0 nssa)
ABR Status...............................Disable
ASBR Status..............................Disable
Stub Router..............................FALSE
External LSDB Overflow..................FALSE

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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 &quot;active&quot; OSPF area is an area with at least one interface up.</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>Maximum Paths</td>
<td>The maximum number of paths that OSPF can report for a given destination.</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>
<tr>
<td>Source</td>
<td>The source protocol/routes that are being redistributed. Possible values are static, connected, or RIP.</td>
</tr>
<tr>
<td>Tag</td>
<td>The decimal value attached to each external route.</td>
</tr>
<tr>
<td>Subnets</td>
<td>For redistributing routes into OSPF, the scope of redistribution for the specified protocol.</td>
</tr>
<tr>
<td>Distribute-List</td>
<td>The access list used to filter redistributed routes.</td>
</tr>
</tbody>
</table>
show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.

Format      show ip ospf abr
Mode

- Privileged EXEC
- User EXEC

<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>

show ip ospf area

This command displays information about the area. The <areaid> identifies the OSPF area that is being displayed.

Format      show ip ospf area <areaid>
Modes

- Privileged EXEC
- User EXEC

<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>
</tbody>
</table>
### ProSafe Managed Switch

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.</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>

**show ip ospf asbr**

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR). This command takes no options.

**Format**

```
show ip ospf asbr
```

**Mode**

- Privileged EXEC
- User EXEC

---

**Routing Commands**

294
### show ip ospf database

This command displays information about the link state database when OSPF is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional `<areaid>` parameter to display database information about a specific area. Use the optional parameters to specify the type of link state advertisements to display.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>asbr-summary</td>
<td>Use <code>asbr-summary</code> to show the autonomous system boundary router (ASBR) summary LSAs.</td>
</tr>
<tr>
<td>external</td>
<td>Use <code>external</code> to display the external LSAs.</td>
</tr>
<tr>
<td>network</td>
<td>Use <code>network</code> to display the network LSAs.</td>
</tr>
<tr>
<td>nssa-external</td>
<td>Use <code>nssa-external</code> to display NSSA external LSAs.</td>
</tr>
<tr>
<td>opaque-area</td>
<td>Use <code>opaque-area</code> to display area opaque LSAs.</td>
</tr>
<tr>
<td>opaque-as</td>
<td>Use <code>opaque-as</code> to display AS opaque LSAs.</td>
</tr>
<tr>
<td>opaque-link</td>
<td>Use <code>opaque-link</code> to display link opaque LSAs.</td>
</tr>
<tr>
<td>router</td>
<td>Use <code>router</code> to display router LSAs.</td>
</tr>
<tr>
<td>summary</td>
<td>Use <code>summary</code> to show the LSA database summary information.</td>
</tr>
<tr>
<td>adv-router</td>
<td>Use <code>adv-router</code> to show the LSAs that are restricted by the advertising router.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Use <code>self-originate</code> 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**

```plaintext
```

**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>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>

**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.

<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 OSPFv3 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>
</tbody>
</table>
Routing Commands

ProSafe Managed Switch

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>

**show ip ospf interface**

This command displays the information for the IFO object or virtual interface tables.

**Format**

`show ip ospf interface {<unit/slot/port> | loopback <loopback-id> | vlan <1-4093>}`

**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>Transit Delay Interval</td>
<td>A number representing the OSPF Transit Delay for the specified interface.</td>
</tr>
<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>
</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>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>
</tbody>
</table>

**show ip ospf interface brief**

This command displays brief information for the IFO object or virtual interface tables.

**Format**

`show ip ospf interface brief`

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</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>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>Retransmit Delay Interval</td>
<td>A number representing the OSPF Transit 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>
**show ip ospf interface stats**

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

**Format**

`show ip ospf interface stats <unit/slot/port>`

**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>External LSA Count</td>
<td>The number of external (LS type 5) link-state advertisements in the link-state database.</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>
<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.</td>
</tr>
<tr>
<td></td>
<td>Note: This field only applies 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>
</tbody>
</table>
The command 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>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 only applies 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 only applies 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>
<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>

**show ip ospf neighbor**

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays. The `<ip-address>` is the IP address of the neighbor, and when you specify this, detailed information about the neighbor...
displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

**Format**

```
show ip ospf neighbor [interface <unit/slot/port>] [<ip-address>]
```

**Modes**

- Privileged EXEC
- User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

<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>Neighbor Interface</td>
<td>The interface of the local router in unit/slot/port format.</td>
</tr>
</tbody>
</table>

**State**

The state of the neighboring routers. Possible values are:
- **Down**: initial state of the neighbor conversation - no recent information has been received from the neighbor.
- **Attempt**: no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.
- **Init**: an Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established.
- **2 way**: communication between the two routers is bidirectional.
- **Exchange start**: the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.
- **Exchange**: the router is describing its entire link state database by sending Database Description packets to the neighbor.
- **Loading**: Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.
- **Full**: the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

**Dead Time**

The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

If you specify an IP address for the neighbor router, the following fields display:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Neighbor IP Address</td>
<td>The IP address of the neighbor router.</td>
</tr>
<tr>
<td>Interface Index</td>
<td>The interface ID of the neighbor router.</td>
</tr>
</tbody>
</table>
The following shows example CLI display output for the command.

(Switch) #show ip ospf neighbor 170.1.1.50

Interface.....................................0/17
Neighbor IP Address...........................170.1.1.50
Interface Index...............................17
Area Id.......................................0.0.0.2
Options.......................................0x2
Router Priority...............................1
Dead timer due in (secs)......................15
Up Time.......................................0 days 2 hrs 8 mins 46 secs
State.........................................Full/BACKUP-DR
Events........................................4
Retransmission Queue Length...................0

show ip ospf range

This command displays information about the area ranges for the specified <areaid>. The <areaid> identifies the OSPF area whose ranges are being displayed.

Format                show ip ospf range <areaid>
Modes
  • Privileged EXEC
  • User EXEC
show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

Format: `show ip ospf statistics`

Modes:
- Privileged EXEC
- User EXEC

<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>IP Address</td>
<td>An IP address which represents this area range.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>A valid subnet mask for this area range.</td>
</tr>
<tr>
<td>Lsdb Type</td>
<td>The type of link advertisement associated with this area range.</td>
</tr>
<tr>
<td>Advertisement</td>
<td>The status of the advertisement. Advertisement has two possible settings: enabled or disabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delta T</td>
<td>How long ago the SPF ran. The time is in the format hh:mm:ss, giving the hours, minutes, and seconds since the SPF run.</td>
</tr>
<tr>
<td>SPF Duration</td>
<td>How long the SPF took in milliseconds.</td>
</tr>
<tr>
<td>Reason</td>
<td>The reason the SPF was scheduled. Reason codes are as follows:</td>
</tr>
<tr>
<td></td>
<td>• R - a router LSA has changed</td>
</tr>
<tr>
<td></td>
<td>• N - a network LSA has changed</td>
</tr>
<tr>
<td></td>
<td>• SN - a type 3 network summary LSA has changed</td>
</tr>
<tr>
<td></td>
<td>• SA - a type 4 ASBR summary LSA has changed</td>
</tr>
<tr>
<td></td>
<td>• X - a type 5 or type 7 external LSA has changed</td>
</tr>
</tbody>
</table>

show ip ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format: `show ip ospf stub table`

Modes:
- Privileged EXEC
- User EXEC
Routing Commands

ProSafe Managed Switch

**show ip ospf virtual-link**

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The `<areaid>` parameter identifies the area and the `<neighbor>` parameter identifies the neighbor's Router ID.

**Format**

```
show ip ospf virtual-link <areaid> <neighbor>
```

**Modes**

- Privileged EXEC
- User EXEC

<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>
<tr>
<td>Iftransit Delay Interval</td>
<td>The configured transit delay for the OSPF virtual interface.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>The configured retransmit interval for the OSPF virtual interface.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The configured authentication type of the OSPF virtual interface.</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</td>
</tr>
<tr>
<td>Neighbor State</td>
<td>The neighbor state.</td>
</tr>
</tbody>
</table>
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>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</td>
<td>The neighbor interface of the OSPF virtual interface.</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>
<tr>
<td>Retransmit Interval</td>
<td>The configured retransmit interval for the OSPF virtual interface.</td>
</tr>
<tr>
<td>Transit Delay</td>
<td>The configured transit delay for the OSPF virtual interface.</td>
</tr>
</tbody>
</table>

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 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 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 to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior that 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.
**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 perform only a graceful restart when the restart is planned (that is, when the restart is a result of the initiate failover command).</td>
</tr>
</tbody>
</table>

**no nsf**

Use this command to disable graceful restart for all restarts.

Format: `no nsf`

Modes: OSPF Router Configuration

**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 called 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>
ProSafe Managed Switch

**no nsf restart-interval**

Use this command to revert the grace period to its default value.

**Format**

```
no [ietf] nsf restart-interval
```

**Modes**

OSPF Router Configuration

---

**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 [ietf] helper [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 help a restarting router performing a planned restart.</td>
</tr>
</tbody>
</table>

---

**no nsf helper**

Use this command to disable helpful neighbor functionality for OSPF.

**Format**

```
no nsf [ietf] helper
```

**Modes**

OSPF Router Configuration

---

**nsf helper disable**

Use this command to disable helpful neighbor functionality for OSPF.

---

**Note:**

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
nsf [ietf] 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

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

Routing Information Protocol (RIP) Commands

This section describes the commands you use to view and configure RIP, which is a distance-vector routing protocol that you use to route traffic within a small network.

router rip

Use this command to enter Router RIP mode.

Format: router rip

Mode: Global Config
enable (RIP)

This command resets the default administrative mode of RIP in the router (active).

Default: enabled
Format: enable
Mode: Router RIP Config

no enable (RIP)

This command sets the administrative mode of RIP in the router to inactive.

Format: no enable
Mode: Router RIP Config

ip rip

This command enables RIP on a router interface.

Default: disabled
Format: ip rip
Mode: Interface Config

no ip rip

This command disables RIP on a router interface.

Format: no ip rip
Mode: Interface Config

auto-summary

This command enables the RIP auto-summarization mode.

Default: disabled
Format: auto-summary
Mode: Router RIP Config

no auto-summary

This command disables the RIP auto-summarization mode.

Format: no auto-summary
Mode: Router RIP Config
default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format  default-information originate
Mode    Router RIP Config

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

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

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

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

no distance rip

This command sets the default route preference value of RIP in the router.

Format  no distance rip
Mode    Router RIP Config
**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

**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

**ip rip authentication**

This command sets the RIP Version 2 Authentication Type and Key for the specified interface. The value of `<type>` is either `none`, `simple`, or `encrypt`. The value for authentication key `<key>` must be 16 bytes or less. The `<key>` is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the value of `<type>` is `encrypt`, a keyid in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID.

Default none

**Format**

```
ip rip authentication {none | {simple <key>} | {encrypt <key> <keyid>}}
```

**Mode**

Interface Config

**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

**ip rip receive version**

This command configures the interface 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

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

ip rip send version

This command configures the interface 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: rip1

Format: ip rip send version {rip1 | rip1c | rip2 | none}

Mode: Interface Config

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

hostroutesaccept

This command enables the RIP hostroutesaccept mode.

Default: enabled

Format: hostroutesaccept

Mode: Router RIP Config
no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format: no hostroutesaccept
Mode: Router RIP Config

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

no split-horizon

This command sets the default RIP split horizon mode.

Format: no split-horizon
Mode: Router RIP Config

redistribute (RIP)

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match <match-type> the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

Default:
- metric—not-configured
- match—internal

Format for OSPF as source protocol:
redistribute ospf [metric <0-15>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]

Format for other source protocol:
redistribute [static | connected] [metric <0-15>]

Mode: Router RIP Config
**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

**show ip rip**

This command displays information relevant to the RIP router.

**Format**

```
show ip rip
```

**Modes**

- Privileged EXEC
- User EXEC

<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>

**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
### show ip rip interface

This command displays information related to a particular RIP interface.

**Format**

```
show ip rip interface {<unit/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>Valid slot and port number separated by forward slashes. 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. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.</td>
</tr>
<tr>
<td>Receive Version</td>
<td>The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.</td>
</tr>
<tr>
<td>RIP Admin Mode</td>
<td>RIP administrative mode of router RIP operation; enable activates, disable de-activates it. 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>
<tr>
<td>Default Metric</td>
<td>A number which represents the metric used for default routes in RIP updates originated on the specified interface. 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>
</tbody>
</table>
ICMP Throttling Commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

**ip unreachables**

Use this command to enable the generation of ICMP Destination Unreachable messages. By default, the generation of ICMP Destination Unreachable messages is enabled.

<table>
<thead>
<tr>
<th>Default</th>
<th>enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip unreachables</td>
</tr>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**no ip unreachables**

Use this command to prevent the generation of ICMP Destination Unreachable messages.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip unreachables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**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 disabled.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip redirects</td>
</tr>
</tbody>
</table>
| Mode      | • Global Config  
            • Interface Config |

**no ip redirects**

Use this command to prevent the generation of ICMP Redirect messages by the router.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip redirects</th>
</tr>
</thead>
</table>
| Mode              | • Global Config  
            • Interface Config |
**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**
- enabled

**Format**
- ip icmp echo-reply

**Mode**
- Global Config

**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

**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

**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
This chapter describes the IP Multicast commands available in the managed switch CLI.

**Note:** Commands described in this chapter that require a license are:
- Multicast Commands
- DVMRP Commands
- PIM Commands
- Internet Group Message Protocol (IGMP) Commands
- IGMP Proxy Commands

This chapter contains the following sections:

- Multicast Commands
- DVMRP Commands
- PIM Commands
- Internet Group Message Protocol (IGMP) Commands
- IGMP Proxy Commands

The commands in this chapter are in 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.

**Multicast Commands**

This section describes the commands you use to configure IP Multicast and to view IP Multicast settings and statistics.
**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.

**Format**

```
ip mcast boundary <groupipaddr> <mask>
```

**Mode**

Interface Config

**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

**ip multicast**

This command sets the administrative mode of the IP multicast forwarder in the router to active.

**Default**

disabled

**Format**

```
ip multicast
```

**Mode**

Global Config

**no ip multicast**

This command sets the administrative mode of the IP multicast forwarder in the router to inactive.

**Format**

```
no ip multicast
```

**Mode**

Global Config

**ip multicast ttl-threshold**

This command is specific to IPv4. Use this command to apply the given Time-to-Live threshold value <ttlthreshold> to a routing interface. The <ttlthreshold> 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 below the configured value are dropped. The value for `<ttlthreshold>` ranges from 0 to 255.

Default: 1

Format: `ip multicast ttl-threshold <ttlvalue>`

Mode: Interface Config

**no ip multicast ttl-threshold**

This command applies the default `<ttlthreshold>` to a routing interface. The `<ttlthreshold>` is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Format: `no ip multicast ttl-threshold`

Mode: Interface Config

**ip mroute**

This command configures an IPv4 Multicast Static Route for a Source.

- `src-addr` is Source IP address of a multicast source or source IP route prefix.
- `src-mask` is Mask associated with the source IP address or source IP route prefix.
- `rpf-addr` is IP address to be used as the RPF address. The interface associated with this IP address, thus, is used as the incoming interface for the mroute.
- `preference` is Administrative distance for the mroute. The lower values have better preference. If the static mroute has the same distance as the other RPF sources, the static mroute will take precedence. The range is from 0 to 255. The default is 0.

Default: No MRoute is configured on the system

Format: `ip mroute <src-addr> <src-mask> <rpf-addr> <preference>`

Mode: Global Config

**no ip mroute**

This command removes the configured IP Multicast Static Route.

Format: `no ip mroute <src-addr>`

Mode: Global Config
**show ip mcast**

This command displays the system-wide multicast information.

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip mcast</th>
</tr>
</thead>
</table>
| 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>
<tr>
<td>Protocol State</td>
<td>The current state of the multicast protocol. Possible values are Operational or Non-Operational.</td>
</tr>
<tr>
<td>Table Max Size</td>
<td>The maximum number of entries allowed in the multicast table.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The multicast protocol running on the router. Possible values are PIM-DM, PIM-SM, or DVMRP.</td>
</tr>
<tr>
<td>Multicast Forwarding Cache Entry Count</td>
<td>The number of entries in the multicast forwarding cache.</td>
</tr>
</tbody>
</table>

**show ip mcast boundary**

This command displays all the configured administrative scoped multicast boundaries.

| Format                  | show ip mcast boundary {<unit/slot/port> | all} |
|-------------------------|------------------------------------------|
| Modes                   | • Privileged EXEC  
|                         | • User EXEC |

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Group Ip</td>
<td>The group IP address.</td>
</tr>
<tr>
<td>Mask</td>
<td>The group IP mask.</td>
</tr>
</tbody>
</table>

**show ip mcast interface**

This command displays the multicast information for the specified interface.

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip mcast interface &lt;unit/slot/port&gt;</th>
</tr>
</thead>
</table>
| Modes                   | • Privileged EXEC  
|                         | • User EXEC |
show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Format    show ip mcast mroute {detail | summary}

Modes
• Privileged EXEC
• User EXEC

If you use the detail parameter, the command displays the following fields:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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>
**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</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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>

**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 | detail}
```

**Modes**

- Privileged EXEC
- User EXEC

If you use the `detail` 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</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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>

**DVMRP Commands**

This section provides a detailed explanation of the Distance Vector Multicast Routing Protocol (DVMRP) commands.

`ip dvmrp (Global Config)`

This command sets administrative mode of DVMRP in the router to active.

- **Default**: disabled
- **Format**: `ip dvmrp`
- **Mode**: Global Config

`no ip dvmrp (Global Config)`

This command sets administrative mode of DVMRP in the router to inactive.

- **Format**: `no ip dvmrp`
- **Mode**: Global Config

`ip dvmrp metric`

This command configures the metric for an interface. 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
**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
```

**ip dvmrp trapflags**

This command enables the DVMRP trap mode.

**Default**
```
disabled
```

**Format**
```
ip dvmrp trapflags
```

**Mode**
```
Global Config
```

**no ip dvmrp trapflags**

This command disables the DVMRP trap mode.

**Format**
```
no ip dvmrp trapflags
```

**Mode**
```
Global Config
```

**ip dvmrp**

This command sets the administrative mode of DVMRP on an interface to active.

**Default**
```
disabled
```

**Format**
```
ip dvmrp
```

**Mode**
```
Interface Config
```

**no ip dvmrp**

This command sets the administrative mode of DVMRP on an interface to inactive.

**Format**
```
no ip dvmrp
```

**Mode**
```
Interface Config
```

**show ip dvmrp**

This command displays the system-wide information for DVMRP.

**Format**
```
show ip dvmrp
```

**Modes**
- Privileged EXEC
- User EXEC
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>Valid slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Interface-Mode</td>
<td>The mode of this interface. Possible values are Enabled and Disabled.</td>
</tr>
<tr>
<td>Operational-status</td>
<td>The current state of DVMRP on this interface. Possible values are</td>
</tr>
<tr>
<td></td>
<td>Operational or Non-Operational.</td>
</tr>
</tbody>
</table>

**show ip dvmrp interface**

This command displays the interface information for DVMRP on the specified interface.

**Format**

`show ip dvmrp interface <unit/slot/port>`

**Modes**

- Privileged EXEC
- User EXEC

The following field is displayed only when DVMRP is operational on the interface.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation ID</td>
<td>The Generation ID value for the interface. This is used by the neighboring</td>
</tr>
<tr>
<td></td>
<td>routers to detect that the DVMRP table should be resent.</td>
</tr>
</tbody>
</table>

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>
</tbody>
</table>
**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>
<tr>
<td>Rcvd Bad Routes</td>
<td>The number of correct packets received with invalid routes.</td>
</tr>
</tbody>
</table>

**show ip dvmrp nexthop**

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

**Format**

```
show ip dvmrp nexthop
```

**Modes**

- Privileged EXEC
- User EXEC
show ip dvmrp prune

This command displays the table listing the router's upstream prune information.

Format: show ip dvmrp prune
Modes:
- Privileged EXEC
- User EXEC

<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>

show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Format: show ip dvmrp route
Modes:
- Privileged EXEC
- User EXEC

<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>
This section describes the commands you use to configure Protocol Independent Multicast (PIM). PIM is a multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol.

**ip pim dense (Global Config)**

This command enables the administrative mode of PIM-DM in the router.

- **Default**: Disabled
- **Format**: `ip pim dense`
- **Mode**: Global Config

**no ip pim dense (Global Config)**

This command disables the administrative mode of PIM-DM in the router.

- **Format**: `no ip pim dense`
- **Mode**: Global Config

**ip pim (Interface Config)**

This command sets administrative mode of PIM on an interface to enabled.

- **Default**: disabled
- **Format**: `ip pim`
- **Mode**: Interface Config

**no ip pim (Interface Config)**

This command sets administrative mode of PIM on an interface to disabled.

- **Format**: `no ip pim`
- **Mode**: Interface Config
**ip pim hello-interval**

This command configures the transmission frequency of PIM Hello messages between PIM enabled neighbors. This field has a range of 0 to 18000 seconds.

**Default**
30

**Format**
`ip pim hello-interval <0-18000>

**Mode**
Interface Config

**no ip pim hello-interval**

This command resets the transmission frequency of hello messages between PIM enabled neighbors to its default value.

**Format**
`no ip pim hello-interval`

**Mode**
Interface Config

**show ip pim interface**

This command displays the PIM Interface status parameters. If the interface number is not specified, this command displays the status parameters of all the PIM enabled interfaces.

**Format**
`show ip pim interface <unit/slot/port>`

**Modes**
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Active PIM protocol</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface number.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Hello interval value. 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>Join-prune interval value.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>DR Priority configured on this Interface. This is not applicable if the interface mode is Dense</td>
</tr>
<tr>
<td>BSR Border</td>
<td>Is this interface configured as a BSR Border?</td>
</tr>
<tr>
<td>Neighbor Count</td>
<td>Number of PIM Neighbors learnt on this interface. This field is displayed only when the interface is operational.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>IP Address of the elected DR on the Interface. This field is displayed only when the interface is Operational.</td>
</tr>
</tbody>
</table>

Example 1:
(Switch) #show ip pim interface
Interface 1/0/1
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

Example 2:
(Switch) #show ip pim interface
Interface 1/0/1
Mode Dense
Hello Interval (secs) 30
Join Prune Interval (secs) 60
DR Priority NA
BSR Border Disabled
Neighbor Count 1
Designated Router NA

show ip pim neighbor

This command displays the neighbor information for PIM on the specified interface.

Format
show ip pim neighbor <unit/slot/port>

Modes
Privileged 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.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface number. Valid slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>UpTime</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>DR Priority configured on this Interface [ PIM -SM only ].</td>
</tr>
</tbody>
</table>

(Switch) #show ip pim neighbor 1/0/1
Neighbor Addr Interface Uptime Expiry Time DR
(19:10:22) (00:02:55 00:01:15 NA)

(Switch) #show ip pim neighbor
Neighbor Addr Interface Uptime Expiry Time DR
(19:10:22) (00:02:55 00:01:15 1)
(19:10:22) (00:03:50 00:02:10 1)
**ip pim sparse (Global Config)**

This command is used to administratively enable PIM Sparse Mode (PIM-SM) multicast routing mode on the router.

**Default**

*disabled*

**Format**

`ip pim sparse`

**Mode**

Global Config

---

**no ip pim sparse (Global Config)**

This command is used to administratively disable PIM-SM multicast routing mode on the router.

**Format**

`no ip pim sparse`

**Mode**

Global Config

---

**ip pim bsr-border**

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

**Default**

*disabled*

**Format**

`ip pim bsr-border`

**Mode**

Interface Config

---

**no ip pim bsr-border**

Use this command to disable the interface from being the BSR border.

**Format**

`no ip pim bsr-border`

**Mode**

Interface Config

---

**ip pim bsr-candidate**

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

**Default**

*None*

**Format**

`ip pim bsr-candidate [interface <interface-num> [hash-mask length] [bsr-priority]]`

**Mode**

Global Config
**ProSafe Managed Switch**

### IP Multicast Commands

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>bar-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 IP address is the BSR. The default value is 0.</td>
</tr>
</tbody>
</table>

**no ip pim bsr-candidate**

This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

**Format**

```
no ip pim bsr-candidate {interface <interface-num> [hash-mask length] [bsr-priority]}
```

**Mode**

Global Config

**ip pim dr-priority**

Use this command to set the priority value for which a router is elected as the designated router (DR).

**Default**

1

**Format**

```
ip pim dr-priority <0-2147483647>
```

**Mode**

Interface Config

**no ip pim dr-priority**

Use this command to disable the interface from being the BSR border.

**Format**

```
no ip pim dr-priority
```

**Mode**

Interface Config

**ip pim join-prune-interval**

This command is used to configure the interface join/prune interval for the PIM router. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

**Default**

60

**Format**

```
ip pim join-prune-interval <0-18000>
```

**Mode**

Interface Config
**no ip pim join-prune-interval**

Use this command to set the join/prune interval to the default value.

**Format**

```plaintext
no ip pim join-prune-interval
```

**Mode**

```
Interface Config
```

**ip pim register-rate-limit**

This command configures the Register Threshold rate for the Rendezvous Point router to switch to a source-specific shortest path. The valid values are from (0 to 2000 kilobits/sec).

**Default**

```
0
```

**Format**

```plaintext
ip pim register-rate-limit <0-2000>
```

**Mode**

```
Global Config
```

**no ip pim register-rate-limit**

This command resets the register threshold rate for the Rendezvous Pointer router to the default value.

**Format**

```plaintext
no ip pim register-rate-limit
```

**Mode**

```
Global Config
```

**ip pim rp-address**

This command is used to statically configure the RP address for one or more multicast groups. The parameter `<rp-address>` is the IP address of the RP. The parameter `<groupaddress>` is the group address supported by the RP. The parameter `<groupmask>` is the group mask for the group address. The optional keyword `override` indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

**Default**

```
disabled
```

**Format**

```plaintext
ip pim rp-address <rp-address> <group-address> <group-mask> [override]
```

**Mode**

```
Global Config
```

**no ip pim rp-address**

This command is used to statically remove the RP address for one or more multicast groups.

**Format**

```plaintext
no ip pim rp-address <rp-address> <group-address> <group-mask> [override]
```

**Mode**

```
Global Config
```
**ip 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).

**Default**

None

**Format**

```
ip pim rp-candidate interface <interface-num> <group-address> <group-mask>
```

**Mode**

Global Config

**no ip 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**

```
o ip pim rp-candidate interface <interface-num> <group-address> <group-mask>
```

**Mode**

Global Config

**ip pim spt-threshold**

This command is used to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The rate is specified in Kilobits per second. The possible values are 0 to 2000.

**Default**

0

**Format**

```
ip pim spt-threshold <0-2000>
```

**Mode**

Global Config

---

**Note:** Non-Zero Data Threshold Rate is currently not supported on this platform. Only Switch on First Packet policy is supported.

---

**no ip pim spt-threshold**

This command is used to set the Data Threshold rate for the RP router to the default value.

**Format**

```
o ip pim spt-threshold
```

**Mode**

Global Config
**ip pim ssm**

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

- **Default**: disabled
- **Format**: `ip pim ssm {default | <group-address> <group-mask>}`
- **Mode**: Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-range</td>
<td>Defines the SSM range access list to 232/8.</td>
</tr>
</tbody>
</table>

**no ip pim ssm**

This command is used to disable the Source Specific Multicast (SSM) range.

- **Format**: `no ip pim ssm {default | <group-address> <group-mask>}`
- **Mode**: Global Config

**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

**no ip pim-trapflags**

This command sets the PIM trap mode to the default.

- **Format**: `no ip pim-trapflags`
- **Mode**: Global Config

**show ip pim**

This command displays the system-wide information for PIM (global configuration mode and interface status).

- **Format**: `show ip pim`
- **Modes**: Privileged EXEC
### PIM Mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Threshold Rate</td>
<td>Rate (in kbps) of SPT Threshold.</td>
</tr>
<tr>
<td>Register Rate-limit</td>
<td>Rate (in kbps) of Register Threshold.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface number.</td>
</tr>
<tr>
<td>Interface-Mode</td>
<td>Enable status of the interface.</td>
</tr>
<tr>
<td>Operational-Status</td>
<td>Operational Status of the Interface.</td>
</tr>
</tbody>
</table>

Example 1:
(Switch) #show ip pim
PIM Mode Dense
Data Threshold Rate (kbps) 0
Register Rate-limit (kbps) 0

Interface Interface-Mode Operational-Status
--------- -------------- ------------------
1/0/1 Enabled Operational
1/0/3 Disabled Non-Operational

Example 2:
(Switch) #show ip pim
PIM Mode Sparse
Data Threshold Rate (kbps) 500
Register Rate-limit (kbps) 100
Interface Interface-Mode Operational-Status
--------- -------------- ------------------
1/0/1 Enabled Operational
1/0/3 Disabled Non-Operational

### show ip pim ssm

This command shows the configured source specific IP multicast addresses.

**Format**

```
show ip pim ssm
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The address of the SSM Group.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Prefix Length of the SSM Group.</td>
</tr>
</tbody>
</table>

(Switch) #show ip pim ssm
Group Address/Prefix Length
--------------------------------
232.0.0.0/8

---

**IP Multicast Commands**

337
**Show ip pim bsr-router**

This command displays the bootstrap router (BSR) information. The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

**Format**  
show ip 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>IP address of the BSR.</td>
</tr>
<tr>
<td>BSR Priority</td>
<td>For candidate it is the configured priority and for elected BSR it is the learned priority.</td>
</tr>
<tr>
<td>BSR Hash Mask Length</td>
<td>Configured or learned hash mask length of the BSR.</td>
</tr>
<tr>
<td>Next Bootstrap message</td>
<td>Time (in hours, minutes, and seconds) in which to send the next bootstrap message from this BSR.</td>
</tr>
<tr>
<td>Next Candidate RP Advertisement in</td>
<td>Time (in hours, minutes, and seconds) in which the next CRP advertisement will be sent. This field is applicable only for the elected RP.</td>
</tr>
</tbody>
</table>

(Switch) # show ip pim bsr-router candidate  
BSR Address 192.168.10.1  
BSR Priority 0  
BSR Hash Mask Length 32  
Next Bootstrap message (hh:mm:ss) NA  
Next Candidate RP Advertisement (hh:mm:ss) NA  

(Switch) # show ip pim bsr-router elected  
BSR Address 192.168.10.1  
BSR Priority 0  
BSR Hash Mask Length 32  
Next Bootstrap message (hh:mm:ss) 00:00:05  
Next Candidate RP Advertisement (hh:mm:ss) 00:00:02

**Show ip pim rp-hash**

This command displays the rendezvous point selected for the specified group address.

**Format**  
show ip pim rp-hash <group-address>

**Modes**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>Address of the RP for the group specified.</td>
</tr>
<tr>
<td>Type</td>
<td>Origin from where this group mapping is learned.</td>
</tr>
</tbody>
</table>

(Switch) # show ip pim rp-hash 224.1.2.0  
RP Address 192.168.10.1  
Type Static
**show ip pim rp mapping**

This command displays the mappings for the PIM group to the active rendezvous points.

**Format**

`show ip pim rp mapping [<rp address> | candidate | static]`

**Modes**

Privileged 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>Address of the multicast group</td>
</tr>
<tr>
<td>Group Mask</td>
<td>Mask for the group address.</td>
</tr>
<tr>
<td>Origin</td>
<td>Origin from where this group mapping is learned.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Expiry time of the elected RP.</td>
</tr>
</tbody>
</table>

**Example:1**

(Switch) #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
Expiry Time (hh:mm:ss) NA

**Example:2**

(Switch) #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
Expiry Time (hh:mm:ss) NA
RP Address 192.168.20.1
Group Address 229.2.0.0
Group Mask 255.255.0.0
Origin Static
Expiry Time (hh:mm:ss) NA

**Example:3**

(Switch) #show ip pim rp mapping candidate
RP Address 192.168.10.1
Group Address 224.1.2.1
Group Mask 255.255.255.0
Origin BSR
Expiry Time (hh:mm:ss) 00:00:08

**Example:4**

(Switch) #show ip pim rp mapping static
Internet Group Message Protocol (IGMP) Commands

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

**ip igmp**

This command sets the administrative mode of IGMP in the system to active.

- **Default**: disabled
- **Format**: `ip igmp`
- **Modes**: • Global Config
  • Interface Config

**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

**ip igmp version**

This command configures the version of IGMP for an interface. The value for `<version>` is either 1, 2 or 3.

- **Default**: 3
- **Format**: `ip igmp version <version>`
- **Modes**: Interface Config

**no ip igmp version**

This command resets the version of IGMP to the default value.

- **Format**: `no ip igmp version`
- **Modes**: Interface Config
**ip igmp last-member-query-count**

This command sets the number of Group-Specific Queries sent 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

**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

**ip igmp last-member-query-interval**

This command configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages. The range for `<seconds>` is 0 to 255 tenths of a second.

**Default**

10 tenths of a second (1 second)

**Format**

```
ip igmp last-member-query-interval <seconds>
```

**Modes**

Interface Config

**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

**ip igmp query-interval**

This command configures the query interval for the specified interface. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for `<queryinterval>` is 1 to 3600 seconds.

**Default**

125 seconds

**Format**

```
ip igmp query-interval <seconds>
```

**Modes**

Interface Config
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
Mode: Interface Config

ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface. The time interval is specified in tenths of a second. The range for \(<\text{maxresptime}>\) is 0 to 255 tenths of a second.

Default: 100
Format: ip igmp query-max-response-time \(<\text{seconds}>\)
Mode: Interface Config

no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format: no ip igmp query-max-response-time
Mode: Interface Config

ip igmp robustness

This command configures the robustness that allows tuning of the interface. 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 \(<\text{robustness}>\) is 1 to 255.

Default: 2
Format: ip igmp robustness \(<\text{robustness}>\)
Mode: Interface Config

no ip igmp robustness

This command sets the robustness value to default.

Format: no ip igmp robustness
Mode: Interface Config
**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. The range for `<count>` is 1 to 20.

Default: 2

Format: `ip igmp startup-query-count <count>`

Mode: Interface Config

**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

**ip igmp startup-query-interval**

This command sets the interval between General Queries sent on startup on the interface. The time interval value is in seconds. The range for `<interval>` is 1 to 300 seconds.

Default: 31

Format: `ip igmp startup-query-interval <interval>`

Mode: Interface Config

**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

**show ip igmp**

This command displays the system-wide IGMP information.

Format: `show ip igmp`

Modes:
- Privileged EXEC
- User EXEC
**IGMP Admin Mode**
- The administrative status of IGMP. This is a configured value.

**Interface**
- Valid slot and port number separated by forward slashes.

**Interface-Mode**
- Indicates whether IGMP is enabled or disabled on the interface. This is a configured value.

**Operational-Status**
- The current state of IGMP on this interface. Possible values are Operational or Non-Operational.

---

**show ip igmp groups**

This command displays the registered multicast groups on the interface. If [detail] is specified this command displays the registered multicast groups on the interface in detail.

**Format**

```
show ip igmp groups <unit/slot/port> [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>
</tbody>
</table>
### show ip igmp interface

This command displays the IGMP information for the interface.

**Format**
```
show ip igmp interface <unit/slot/port>
```

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</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>
<tr>
<td>Robustness</td>
<td>The tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface.</td>
</tr>
<tr>
<td>Startup Query Interval</td>
<td>The interval between General Queries sent by a Querier on startup.</td>
</tr>
<tr>
<td>Startup Query Count</td>
<td>The number of Queries sent out on startup, separated by the Startup Query Interval.</td>
</tr>
<tr>
<td>Last Member Query Interval</td>
<td>The 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>The number of Group-Specific Queries sent before the router assumes that there are no local members.</td>
</tr>
</tbody>
</table>
**show ip igmp interface membership**

This command displays the list of interfaces that have registered in the multicast group.

**Format**

```
show ip igmp interface membership <multiipaddr> [detail]
```

**Mode**

Privileged EXEC

<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 “-----” 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 “-----” 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 “-----” 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 “-----” for IGMPv1 and IGMPv2 Membership Reports.</td>
</tr>
</tbody>
</table>

**show ip igmp interface stats**

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

**Format**

```
show ip igmp interface stats <unit/slot/port>
```

**Modes**

- Privileged EXEC
- User EXEC
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querier Status</td>
<td>The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.</td>
</tr>
<tr>
<td>Querier IP Address</td>
<td>The IP address of the IGMP Querier on the IP subnet to which this interface is attached.</td>
</tr>
<tr>
<td>Querier Up Time</td>
<td>The time since the interface Querier was last changed.</td>
</tr>
<tr>
<td>Querier Expiry Time</td>
<td>The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.</td>
</tr>
<tr>
<td>Wrong Version Queries</td>
<td>The number of queries received whose IGMP version does not match the IGMP 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 Groups</td>
<td>The current number of membership entries for this interface.</td>
</tr>
</tbody>
</table>

**IGMP Proxy Commands**

The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

**ip igmp-proxy**

This command enables the IGMP Proxy on the router. To enable the IGMP Proxy on the router, you must enable multicast forwarding. Also, make sure that there are no multicast routing protocols enabled on the router.

**Format**  
```yaml
ip igmp-proxy
```

**Mode**  
Interface Config

**no ip igmp-proxy**

This command disables the IGMP Proxy on the router.

**Format**  
```yaml
no ip igmp-proxy
```

**Mode**  
Interface Config
ip igmp-proxy unsolicit-rprt-interval

This command sets the unsolicited report interval for the IGMP Proxy router. This command is valid only when you enable IGMP Proxy on the interface. The value of <interval> can be 1-260 seconds.

Default 1
Format ip igmp-proxy unsolicit-rprt-interval <interval>
Mode Interface Config

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

ip igmp-proxy reset-status

This command resets the host interface status parameters of the IGMP Proxy router. This command is valid only when you enable IGMP Proxy on the interface.

Format ip igmp-proxy reset-status
Mode Interface Config

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>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(Switch) #show ip igmp-proxy

Interface Index............................................. 1/0/1
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

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 unit/slot/port of the IGMP proxy.</td>
</tr>
</tbody>
</table>

The column headings of the table associated with the interface are as follows:
ProSafe Managed Switch

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

(Switch) #show ip igmp-proxy interface

<table>
<thead>
<tr>
<th>Interface Index</th>
<th>1/0/1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ver</td>
<td>1</td>
</tr>
<tr>
<td>Query Rcvd</td>
<td>0</td>
</tr>
<tr>
<td>Report Rcvd</td>
<td>0</td>
</tr>
<tr>
<td>Report Sent</td>
<td>0</td>
</tr>
<tr>
<td>Leave Rcvd</td>
<td>-----</td>
</tr>
<tr>
<td>Leave Sent</td>
<td>-----</td>
</tr>
</tbody>
</table>

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.

<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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Format</th>
<th>show ip igmp-proxy groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modes</td>
<td>Privileged EXEC</td>
</tr>
<tr>
<td></td>
<td>User EXEC</td>
</tr>
</tbody>
</table>

IP Multicast Commands
350
Example: The following shows example CLI display output for the command.

(Switch) #show ip igmp-proxy groups

Interface Index............................. 1/0/1

<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>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>

**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.

<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>
<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.

(Switch) #show ip igmp-proxy groups

Interface Index......................... 1/0/1

<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>
<th>Group Source List</th>
<th>Expiry Time</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>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Group Source List

| 5.1.2.3       | 00:02:21     |
| 6.1.2.3       | 00:02:21     |
| 7.1.2.3       | 00:02:21     |

| 226.4.4.4     | 5.5.5.48      | 00:02:21  | DELAY_MEMBER | Include      | 3       |                   |             |

Group Source List

| 2.1.2.3       | 00:02:21     |
| 6.1.2.3       | 00:01:44     |
| 8.1.2.3       | 00:01:44     |

| 227.4.4.4     | 5.5.5.48      | 00:02:21  | DELAY_MEMBER | Exclude      | 0       |                   |             |

| 228.4.4.4     | 5.5.5.48      | 00:03:21  | DELAY_MEMBER | Include      | 3       |                   |             |

Group Source List

| 9.1.2.3       | 00:03:21     |
| 6.1.2.3       | 00:03:21     |
| 7.1.2.3       | 00:03:21     |
This chapter describes the IPv6 commands available in the managed switch CLI.

**Note:** Commands described in this chapter that require a license are:
- Tunnel Interface Commands
- IPv6 Routing Commands
- OSPFv3 Commands
- OSPFv3 Graceful Restart Commands
- DHCPv6 Commands

This chapter contains the following sections:
- Tunnel Interface Commands
- IPv6 Routing Commands
- OSPFv3 Commands
- OSPFv3 Graceful Restart Commands
- DHCPv6 Commands

The commands in this chapter are in 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.

**Note:** For information on IPv6 management commands, see IPv6 Management Commands on page 659.
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 238. To assign an IPv6 address to the tunnel interface, see `ipv6 address` on page 357.

`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

`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

`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 <unit/slot/port>}
```

**Mode**

Interface Config

`tunnel destination`

This command specifies the destination transport address of the tunnel.

**Format**

```
tunnel destination {<ipv4-address>}
```

**Mode**

Interface Config
**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

**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>
<tr>
<td>MTU Size</td>
<td>The maximum transmission unit for packets on the interface.</td>
</tr>
<tr>
<td>IPv6 Prefix is</td>
<td>If you enable IPv6 on the interface and assign an address, the IPv6 address and prefix display.</td>
</tr>
</tbody>
</table>

**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.
**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

**no ipv6 hop-limit**

This command returns the unicast hop count to the default.

**Format**
no ipv6 hop-limit

**Mode**
Global Config

**ipv6 unicast-routing**

Use this command to enable the forwarding of IPv6 unicast datagrams.

**Default**
disabled

**Format**
ipv6 unicast-routing

**Mode**
Global Config

**no ipv6 unicast-routing**

Use this command to disable the forwarding of IPv6 unicast datagrams.

**Format**
no ipv6 unicast-routing

**Mode**
Global Config

**ipv6 enable**

Use this command to enable IPv6 routing on an interface, 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
no ipv6 enable

Use this command to disable IPv6 routing on an interface.

Format          no ipv6 enable
Mode            Interface Config

ipv6 address

Use this command to configure an IPv6 address on an interface, 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:f101:0:0:0:1 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

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
**ipv6 address autoconfig**

This command is used to enable stateless address autoconfiguration capability.

**Note:** When unicast-routing is enabled, autoconfig mode doesn’t work.

**Format**

```
ipv6 address autoconfig
```

**Mode**

```
Interface Config
```

**ipv6 address autoconfig**

This command disables the stateless autoconfiguration.

**Format**

```
no ipv6 address autoconfig
```

**Mode**

```
Interface Config
```

**ipv6 address dhcp**

This command is used to enable DHCPv6 client capability.

**Format**

```
ipv6 address autoconfig
```

**Mode**

```
Interface Config
```

**no ipv6 address dhcp**

The "no" form of this command disables the DHCPv6 client capability.

**Format**

```
no ipv6 address autoconfig
```

**Mode**

```
Interface Config
```

**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. You can specify a `<unit/slot/port>` 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 {<unit/slot/port> | tunnel <tunnel_id>} <next-hop-address>} [<preference>]`

**Mode**  
Global Config

**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 {<unit/slot/port> | tunnel <tunnel_id>} <next-hop-address> | <preference>}]`

**Mode**  
Global Config

**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

**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
**ipv6 mtu**

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface. This command replaces the default or link MTU with a new MTU value.

**Note:** 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

**no ipv6 mtu**

This command resets maximum transmission unit value to default value.

**Format**

```
no ipv6 mtu
```

**Mode**

Interface Config

**ipv6 nd dad attempts**

This command sets the number of duplicate address detection probes transmitted. 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

**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
**ipv6 nd managed-config-flag**

This command sets the "managed address configuration" flag in router advertisements. 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

**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

**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.

**Default**
0

**Format**
ipv6 nd ns-interval <1000-4294967295> | 0

**Mode** Interface Config

**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

**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
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

ipv6 nd ra-interval

This command sets the transmission interval between router advertisements.

Default  600
Format  ipv6 nd ra-interval-max <4- 1800>
Mode     Interface Config

no ipv6 nd ra-interval

This command sets router advertisement interval to the default.

Format  no ipv6 nd ra-interval-max
Mode     Interface Config

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. The \(<\text{lifetime}>\) 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

no ipv6 nd ra-lifetime

This command resets router lifetime to the default value.

Format  no ipv6 nd ra-lifetime
Mode     Interface Config
**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.

**Default**

0

**Format**

`ipv6 nd reachable-time <0-3600000>`

**Mode**

Interface Config

**no ipv6 nd reachable-time**

This command means reachable time is unspecified for the router.

**Format**

`no ipv6 nd reachable-time`

**Mode**

Interface Config

**ipv6 nd suppress-ra**

This command suppresses router advertisement transmission on an interface.

**Default**

`disabled`

**Format**

`ipv6 nd suppress-ra`

**Mode**

Interface Config

**no ipv6 nd suppress-ra**

This command enables router transmission on an interface.

**Format**

`no ipv6 nd suppress-ra`

**Mode**

Interface Config

**ipv6 nd router-preference**

This is used to configure router preference value in IPv6 router advertisements on an interface. This will indicate whether or not to prefer this router over other default routers.

**Default**

`Medium`

**Format**

`ipv6 nd router-preference <high/low/medium>`

**Mode**

Interface Config
**ipv6 nd router-preference**

This command will set the router preference to default.

**Format**

```text
no ipv6 router-preference
```

**Mode**

Interface Config

**ipv6 unreachables**

Use this command to enable the generation of ICMPv6 Destination Unreachable messages. By default, the generation of ICMPv6 Destination Unreachable messages is enabled.

**Default**

enable

**Format**

```text
ipv6 unreachables
```

**Mode**

Interface Config

**no ipv6 unreachables**

Use this command to prevent the generation of ICMPv6 Destination Unreachable messages.

**Format**

```text
no ipv6 unreachables
```

**Mode**

Interface Config

**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).

**Default**

- `burst-interval` of 1000 msec.
- `burst-size` of 100 messages

**Format**

```text
ipv6 icmp error-interval <burst-interval> [<burst-size>]
```

**Mode**

Global Config
**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

**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 <code>ipv6 hop-limit</code> on page 356.</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 <code>ipv6 icmp error-interval</code> on page 364.</td>
</tr>
<tr>
<td>ICMPv6 Rate Limit Burst Size</td>
<td>Shows the number of ICMPv6 error messages that can be sent during one <code>burst-interval</code>. For more information, see <code>ipv6 icmp error-interval</code> on page 364.</td>
</tr>
<tr>
<td>Maximum Routes</td>
<td>Shows the maximum IPv6 route table size.</td>
</tr>
</tbody>
</table>

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

```
(Switch) #show ipv6 brief

IPv6 Forwarding Mode........................... Enable
IPv6 Unicast Routing Mode...................... Enable
IPv6 Hop Limit.................................. 0
ICMPv6 Rate Limit Error Interval.............. 1000 msec
ICMPv6 Rate Limit Burst Size................... 100 messages
Maximum Routes................................. 3000
```
show ipv6 interface

Use this command to show the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent.

**Format**

```
show ipv6 interface {brief | <unit/slot/port> | tunnel <0-7> | loopback <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>Interface</td>
<td>The interface in unit/slot/port format.</td>
</tr>
<tr>
<td>IPv6 Routing Operational Mode</td>
<td>Shows whether the mode is enabled or disabled.</td>
</tr>
<tr>
<td>IPv6 Address/Length</td>
<td>Shows the IPv6 address and length on interfaces with IPv6 enabled.</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>IPv6 is enabled</td>
<td>Appears if IPv6 is enabled on the interface.</td>
</tr>
<tr>
<td>Routing Mode</td>
<td>Shows whether IPv6 routing is enabled or disabled.</td>
</tr>
<tr>
<td>Administrative Mode</td>
<td>Shows whether the interface administrative mode is enabled or disabled.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Shows bandwidth of the interface.</td>
</tr>
<tr>
<td>Interface Maximum Transmission Unit</td>
<td>The MTU size, in bytes.</td>
</tr>
<tr>
<td>Router Duplicate Address Detection Transmits</td>
<td>The number of consecutive duplicate address detection probes to transmit.</td>
</tr>
<tr>
<td>Router Advertisement NS Interval</td>
<td>The interval, in milliseconds, between router advertisements for advertised neighbor solicitations.</td>
</tr>
<tr>
<td>Router Advertisement Lifetime</td>
<td>Shows the router lifetime value of the interface in router advertisements.</td>
</tr>
<tr>
<td>Router Advertisement Reachable Time</td>
<td>The amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.</td>
</tr>
</tbody>
</table>
Example: The following shows example CLI display output for the command.

(Switch) #show ipv6 interface 1/0/1

Routing Mode................................... Disabled
Administrative Mode............................ Enabled
IPv6 Routing Operational Mode.................. Disabled
Bandwidth...................................... 100000 kbps
Interface Maximum Transmit Unit................ 1500
Router Duplicate Address Detection Transmits... 1
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 Suppress Flag............. Disabled
IPv6 Destination Unreachables.................. Enabled

No IPv6 prefixes configured.

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</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>
**show ipv6 neighbor**

Use this command to display information about the IPv6 neighbors.

**Format**

```
show ipv6 neighbor
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface in unit/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 not mean 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>
</tbody>
</table>

**clear ipv6 neighbors**

Use this command to clear all entries IPv6 neighbor table or an entry on a specific interface. Use the `<unit/slot/port>` parameter to specify the interface.

**Format**

```
clear ipv6 neighbors [<unit/slot/port>]
```

**Mode**

Privileged EXEC

**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 `<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 non-best routes are displayed. Otherwise, only the best routes are displayed.

**Note:** If you use the `connected` keyword for `<protocol>`, the `all` option is not available because there are no best or non-best connected routes.
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

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>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>
</tbody>
</table>
| Route-Timestamp  | The last updated time for dynamic routes. The format of Route-Timestamp will be
|                  | • Days:Hours:Minutes if days > 1
|                  | • Hours:Minutes:Seconds if days < 1 |
| Interface        | The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be `Null0` interface. |

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

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

```bash
(Switch) #show ipv6 route
IPv6 Routing Table - 3 entries
```
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

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::200:4fff:fe35:c8bb,  00h:01m:47s,  0/11

**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

<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>

**show ipv6 route summary**

This command displays the summary of the routing table. Use `all` to display the count summary for all routes, including best and non-best routes. Use the command without parameters to display the count summary for only the best routes.

**Format**

```
show ipv6 route summary [all]
```

**Modes**

- Privileged EXEC
- User EXEC
### IPv6 Commands

#### Connected Routes
Total number of connected routes in the routing table.

#### Static Routes
Total number of static routes in the routing table.

#### OSPF Routes
Total number of routes installed by OSPFv3 protocol.

#### Reject Routes
Total number of reject routes installed by all protocols.

#### Number of Prefixes
Summarizes the number of routes with prefixes of different lengths.

#### Total Routes
The total number of routes in the routing 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>
</tbody>
</table>

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

```bash
(Switch) #show ipv6 route summary
IPv6 Routing Table Summary - 3 entries

Connected Routes.......................1
Static Routes............................2
OSPF Routes...............................0
    Intra Area Routes.....................0
    Inter Area Routes.....................0
    External Type-1 Routes..............0
    External Type-2 Routes..............0
Reject Routes.............................1
Total routes.............................3

Number of Prefixes:
    /64: 3
```

**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 unit/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>

**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. If you do not specify an interface, the command displays information about traffic on all interfaces.

**Format**

```
show ipv6 traffic [{<unit/slot/port> | loopback <loopback-id> | tunnel <tunnel-id>}]`n```

**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>Received Datagrams Discarded Due To No Route</td>
<td>Number of input datagrams discarded because no route could be found to transmit them to their destination.</td>
</tr>
<tr>
<td>Received Datagrams With Unknown Protocol</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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Received Datagrams Discarded Due To Invalid Addr</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>Received Datagrams Discarded Due To Truncated</td>
<td>Number of input datagrams discarded because datagram frame didn’t carry enough data.</td>
</tr>
<tr>
<td>Received Datagrams Discarded Other</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>Received Datagrams Reassembly Required</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>Datagrams Successfully Reassembled</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>Datagrams Failed To Reassemble</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>Datagrams Forwarded</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>Datagrams Locally Transmitted</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>Datagrams Transmit Failed</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 met this (discretionary) discard criterion.</td>
</tr>
<tr>
<td>Fragments Created</td>
<td>Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.</td>
</tr>
<tr>
<td>Datagrams Successfully Fragmented</td>
<td>Number of IPv6 datagrams that have been successfully fragmented at this output interface.</td>
</tr>
<tr>
<td>Datagrams Failed To Fragment</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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Multicast Datagrams Received</td>
<td>Number of multicast packets received by the interface.</td>
</tr>
<tr>
<td>Multicast Datagrams Transmitted</td>
<td>Number of multicast packets transmitted by the interface.</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 ipv6IfImpInErrors. Note that this interface is the 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</td>
<td>Number of ICMP Destination Unreachable messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Messages Prohibited Administratively</td>
<td>Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Time Exceeded Messages</td>
<td>Number of ICMP Time Exceeded messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 Parameter Problem Messages</td>
<td>Number of ICMP Parameter Problem messages received by the interface.</td>
</tr>
<tr>
<td>ICMPv6 messages with too big packets</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>Transmitted</td>
<td>Number of ICMPv6 Group Membership Query 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>
</tbody>
</table>
### IPv6 Commands

**ProSafe Managed Switch**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 statistics</td>
<td>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</td>
</tr>
</tbody>
</table>

**IPv6 Commands**

375
**traffic** command. If you do not specify an interface, the counters for all IPv6 traffic statistics reset to zero.

**Format**
```
clear ipv6 statistics [{<unit/slot/port> | loopback <loopback-id> | tunnel <tunnel-id>}]
```

**Mode**
Privileged EXEC

### 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.

**ipv6 ospf**

This command enables OSPF on a router interface or loopback interface.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Format</strong></td>
<td><code>ipv6 ospf</code></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Interface Config</td>
</tr>
</tbody>
</table>

**no ipv6 ospf**

This command disables OSPF on a router interface or loopback interface.

| **Format** | `no ipv6 ospf` |
| **Mode** | Interface Config |

**ipv6 ospf area**

This command sets the OSPF area to which the specified router interface belongs. The `<areaid>` is an IPv6 address, formatted as a 4-digit dotted-decimal number or a decimal value in the range of `<0-4294967295>`. The `<areaid>` uniquely identifies the area to which the interface connects. Assigning an area id, which does not exist on an interface, causes the area to be created with default values.

| **Format** | `ipv6 ospf area <areaid>` |
| **Mode** | Interface Config |
**ipv6 ospf cost**

This command configures the cost on an OSPF interface. The `<cost>` parameter has a range of 1 to 65535.

**Default** 10

**Format** `ipv6 ospf cost <1-65535>`

**Mode** Interface Config

**no ipv6 ospf cost**

This command configures the default cost on an OSPF interface.

**Format** `no ipv6 ospf cost`

**Mode** Interface Config

**ipv6 ospf dead-interval**

This command sets the OSPF dead interval for the specified interface. 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.

**Default** 40

**Format** `ipv6 ospf dead-interval <seconds>`

**Mode** Interface Config

**no ipv6 ospf dead-interval**

This command sets the default OSPF dead interval for the specified interface.

**Format** `no ipv6 ospf dead-interval`

**Mode** Interface Config

**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
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

ipv6 ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. 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

no ipv6 ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format
no ipv6 ospf mtu-ignore

Mode
Interface Config

ipv6 ospf network

This command changes the default OSPF network type for the interface. 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
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

ipv6 ospf priority

This command sets the OSPF priority for the specified router interface. 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

no ipv6 ospf priority

This command sets the default OSPF priority for the specified router interface.

Format: `no ipv6 ospf priority`
Mode: Interface Config

ipv6 ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface. 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

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
ipv6 ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. 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

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

ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Format: ipv6 router ospf
Mode: Global Config

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

area nssa (OSPFv3)

This command configures the specified areaid to function as an NSSA.

Format: area `<areaid>` nssa
Mode: Router OSPFv3 Config
**no area nssa(OSPFv3)**

This command disables nssa from the specified area id.

**Format**

```
no area <areaid> nssa
```

**Mode**

Router OSPFv3 Config

**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 non-comparable (nssa-external 2).

**Format**

```
area <areaid> nssa default-info-originate [<metric>] [{comparable | non-comparable}]
```

**Mode**

Router OSPFv3 Config

**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 OSPF Config

**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

**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 OSPF Config
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

no area nssa no-summary (OSPFv3)

This command disables nssa from the summary LSAs.

Format: no area <areaid> nssa no-summary

Mode: Router OSPF Config

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

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 OSPF Config

area nssa translator-stab-intv (OSPFv3)

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 OSPFv3 Config
**no area nssa translator-stab-intv (OSPFv3)**

This command disables the nssa translator's `<stabilityinterval>` from the specified area id.

**Format**

```bash
no area <areaid> nssa translator-stab-intv <stabilityinterval>
```

**Mode**

Router OSPF Config

**area range (OSPFv3)**

This command creates a specified area range for a specified NSSA. The `<ipaddr>` is a valid IP address. The `<subnetmask>` is a valid subnet mask. The LSDB type must be specified by either `summarylink` or `nssaexternallink`, and the advertising of the area range can be allowed or suppressed.

**Format**

```bash
area <areaid> range <ipv6-prefix> <prefix-length> {summarylink | nssaexternallink} [advertise | not-advertise]
```

**Mode**

Router OSPFv3 Config

**no area range(OSPFv3)**

This command deletes a specified area range. The `<ipaddr>` is a valid IP address. The `<subnetmask>` is a valid subnet mask.

**Format**

```bash
no area <areaid> range <ipv6-prefix> <prefix-length>
```

**Mode**

Router OSPFv3 Config

**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**

```bash
area <areaid> stub
```

**Mode**

Router OSPFv3 Config

**no area stub(OSPFv3)**

This command deletes a stub area for the specified area ID.

**Format**

```bash
no area <areaid> stub
```

**Mode**

Router OSPFv3 Config
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

no area stub no-summary (OSPFv3)

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

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

no area virtual-link (OSPFv3)

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

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
no area virtual-link dead-interval (OSPFv3)

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

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

no area virtual-link hello-interval (OSPFv3)

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

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
no area virtual-link retransmit-interval (OSPFv3)

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

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

no area virtual-link transmit-delay (OSPFv3)

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

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. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

Default: 100Mbps
IPv6 Commands

ProSafe Managed Switch

Format: auto-cost reference-bandwidth <1 to 4294967>
Mode: Router OSPFv3 Config

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

clear ipv6 ospf
Use this command to disable and re-enable OSPF.

Format: clear ipv6 ospf
Mode: Privileged EXEC

clear ipv6 ospf configuration
Use this command to reset the OSPF configuration to factory defaults.

Format: clear ipv6 ospf configuration
Mode: Privileged EXEC

clear ipv6 ospf counters
Use this command to reset global and interface statistics.

Format: clear ipv6 ospf counters
Mode: Privileged EXEC

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


**clear ipv6 ospf neighbor interface**

To drop adjacency with all neighbors on a specific interface, use the optional parameter [unit/slot/port]. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [neighbor-id].

**Format**

clear ipv6 ospf neighbor interface [unit/slot/port] [neighbor-id]

**Mode**

Privileged EXEC

**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

**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 <1-16777214>] [metric-type {1 | 2}]

**Mode**

Router OSPFv3 Config

**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

**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
**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

**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

**no distance ospf(OSPFv3)**

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

**enable (OSPFv3)**

This command resets the default administrative mode of OSPF in the router (active).

**Default**
enabled

**Format**
```
enable
```

**Mode**
Router OSPFv3 Config

**no enable (OSPFv3)**

This command sets the administrative mode of OSPF in the router to inactive.

**Format**
```
no enable
```

**Mode**
Router OSPFv3 Config
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

no exit-overflow-interval (OSPFv3)

This command configures the default exit overflow interval for OSPF.

Format: no exit-overflow-interval
Mode: Router OSPFv3 Config

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 non-default AS-external-LSAs in a router’s link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for <limit> is –1 to 2147483647.

Default: -1
Format: external-lsdb-limit <limit>
Mode: Router OSPFv3 Config

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format: no external-lsdb-limit
Mode: Router OSPFv3 Config
**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

**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

**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

**no passive-interface default (OSPFv3)**

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

**Format**

`no passive-interface default`

**Mode**

Router OSPFv3 Config

**passive-interface (OSPFv3)**

Use this command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

**Default**

disabled

**Format**

`passive-interface (<unit/slot/port> | tunnel <tunnel-id>)`

**Mode**

Router OSPFv3 Config
no passive-interface (OSPFv3)

Use this command to set the interface or tunnel as non-passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

**Format**

```
no passive-interface {<unit/slot/port> | tunnel <tunnel-id>}
```

**Mode**

Router OSPFv3 Config

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

no redistribute (OSPFv3)

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

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
**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 2, Trapflag Groups (OSPFv3)*.

**Table 2. 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>if-rx</td>
<td>ir-rx-packet</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>rtb</td>
<td>• rtb-entry-info</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] |
    if-rx [all | if-rx-packet] |
    lsa [all | lsa-maxage | lsa-originate] |
    overflow [all | lsdb-overflow | lsdb-approaching-overflow] |
    retransmit [all | packets | virt-packets] |
    rtb [all, rtb-entry-info] |
    state-change [all | if-state-change | neighbor-state-change | virtif-state-
    change | virtneighbor-state-change]
  }
```

Mode:

```
  Router OSPFv3 Config
```

no trapflags(OSPFv3)

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the `group name` followed by that particular flag.
- To disable all the flags in that group, give the group name followed by `all`.
- To disable all the flags, give the command as `trapflags all`.

Format:

```
  no trapflags {
    all |
    errors [all | authentication-failure | bad-packet | config-error | virt-
    authentication-failure | virt-bad-packet | virt-config-error] |
    if-rx [all | if-rx-packet] |
    lsa [all | lsa-maxage | lsa-originate] |
    overflow [all | lsdb-overflow | lsdb-approaching-overflow] |
    retransmit [all | packets | virt-packets] |
    rtb [all, rtb-entry-info] |
    state-change [all | if-state-change | neighbor-state-change | virtif-state-
    change | virtneighbor-state-change]
  }
```

Mode:

```
  Router OSPFv3 Config
```

```
show ipv6 ospf
```

This command displays information relevant to the OSPF router.

Format:

```
  show ipv6 ospf
```

Mode:

```
  Privileged EXEC
```

---

**IPv6 Commands**

394
Note: 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>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. 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 re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).</td>
</tr>
<tr>
<td>Stub Router</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 re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.</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>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 number of link-state advertisements received determined to be new instantiations.</td>
</tr>
<tr>
<td>Maximum Number of LSAs</td>
<td>The total number of link state advertisements currently in the link state database.</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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</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>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>Default Metric</td>
<td>Default value for redistributed routes.</td>
</tr>
<tr>
<td>Default Passive Setting</td>
<td>Shows whether the interfaces are passive by default.</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 &quot;active&quot; OSPF area is an area with at least one interface up.</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>Maximum Paths</td>
<td>The maximum number of paths that OSPF can report for a given destination.</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>
<tr>
<td>Source</td>
<td>Shows source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric of the routes being redistributed.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>Shows whether the routes are External Type 1 or External Type 2.</td>
</tr>
<tr>
<td>Tag</td>
<td>The decimal value attached to each external route.</td>
</tr>
<tr>
<td>Subnets</td>
<td>For redistributing routes into OSPF, the scope of redistribution for the specified protocol.</td>
</tr>
<tr>
<td>Distribute-List</td>
<td>The access list used to filter redistributed routes.</td>
</tr>
</tbody>
</table>
**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

<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>

**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>
</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>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>

**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

<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>
</tbody>
</table>
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-originate 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-originate}]
```

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>Options</td>
<td>An integer indicating 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>
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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Total number of router LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Network</td>
<td>Total number of network LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Inter-area Prefix</td>
<td>Total number of inter-area prefix LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Inter-area Router</td>
<td>Total number of inter-area router LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Type-7 Ext</td>
<td>Total number of NSSA external LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Link</td>
<td>Total number of link LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Intra-area Prefix</td>
<td>Total number of intra-area prefix LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Link Unknown</td>
<td>Total number of link-source unknown LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Area Unknown</td>
<td>Total number of area unknown LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>AS Unknown</td>
<td>Total number of as unknown LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Type-5 Ext</td>
<td>Total number of AS external LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Self-Originated Type-5</td>
<td>Total number of self originated AS external LSAs in the OSPFv3 link state database.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of router LSAs in the OSPFv3 link state database.</td>
</tr>
</tbody>
</table>

show ipv6 ospf interface

This command displays the information for the IFO object or virtual interface tables.

Format
show ipv6 ospf interface [<unit/slot/port> | 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>IPv6 Address</td>
<td>The IPv6 address of the interface.</td>
</tr>
<tr>
<td>ifIndex</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>
</tbody>
</table>
### IPv6 Commands

**ProSafe Managed Switch**

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>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>Itransit Delay Interval</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>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>
</tbody>
</table>

**Terms**

- **Broadcast LANs**
  - Such as Ethernet and IEEE 802.5, take the value *broadcast*. The OSPF Interface Type will be 'broadcast'.
  - The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.

**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
show ipv6 ospf interface stats

This command displays the statistics for a specific interface. The command only displays information if OSPF is enabled.

**Format**      show ipv6 ospf interface stats <unit/slot/port>

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>States whether OSPF is enabled or disabled on a router interface.</td>
</tr>
<tr>
<td>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>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>

**show ipv6 ospf interface stats**

This command displays the statistics for a specific interface. The command only displays information if OSPF is enabled.

**Format**      show ipv6 ospf interface stats <unit/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>IPv6 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>
<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>Packets Received</td>
<td>The number of OSPFv3 packets received on the interface.</td>
</tr>
<tr>
<td>Packets Transmitted</td>
<td>The number of OSPFv3 packets sent on the interface.</td>
</tr>
<tr>
<td>LSAs Sent</td>
<td>The total number of LSAs flooded on the interface.</td>
</tr>
</tbody>
</table>
### IPv6 Commands

#### ProSafe Managed Switch

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSA Acks Received</td>
<td>The total number of LSA acknowledged from this interface.</td>
</tr>
<tr>
<td>LSA Acks Sent</td>
<td>The total number of LSAs acknowledged to this interface.</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>
<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>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>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>

See `show ip ospf interface stats` on page 299 for a sample output of the number of OSPF packets of each type sent and received on the interface.

**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 `<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 ipv6 ospf neighbor [interface [unit/slot/port] | tunnel <tunnel_id>] [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>Intf ID</td>
<td>The interface ID of the neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface of the local router in unit/slot/port format.</td>
</tr>
<tr>
<td>State</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>• Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.</td>
</tr>
<tr>
<td>Dead Time</td>
<td>The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.</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>Interface</td>
<td>The interface of the local router in unit/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>
</tbody>
</table>
show ipv6 ospf range

This command displays information about the area ranges for the specified `<areaid>`. The `<areaid>` identifies the OSPF area whose ranges are being displayed.

**Format**
show ipv6 ospf range `<areaid>`

**Modes**
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>

**Term**
<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Lsdb Type</td>
</tr>
<tr>
<td>Advertisement</td>
</tr>
</tbody>
</table>

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>
<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>
**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

**Term**

<table>
<thead>
<tr>
<th>Area ID</th>
<th>The area id of the requested OSPF area.</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Iftransit Delay Interval</td>
<td>The configured transit delay for the OSPF virtual interface.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>The configured retransmit interval for the OSPF 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>

**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

**Term**

<table>
<thead>
<tr>
<th>Area ID</th>
<th>The area id of the requested OSPFV3 area.</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
The managed switch implementation of OSPFv3 supports graceful restart as specified in RFC 5187 and RFC 3623. Graceful restart works together with managed switch non-stop forwarding (nsf) to enable the hardware to continue forwarding IPv6 packets using OSPFv3 routes while a backup unit takes over management unit responsibility. When OSPF executes a graceful restart, it informs its neighbors that the OSPF control plane is restarting but will be back shortly. Helpful neighbors continue to advertise to the network that they have full adjacencies with the restarting router, avoiding announcement of a topology change and related events (for example, flooding of LSAs and SPF runs). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart implements both the restarting router and helpful neighbor features described in RFC 3623.

**nsf (OSPFv3)**

This command enables OSPF graceful restart. The `ietf` parameter is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is not the only one supported, this parameter is optional. The `planned-only` parameter indicates that OSPF performs a graceful restart only when the restart is planned (that is, when the restart results from the `initiate failover` command).

- **Default**: disabled
- **Format**: `nsf [ ietf ] [ planned-only ]`
- **Mode**: OSPFv3 Router Configuration mode

**no nsf [ietf] (OSPFv3)**

This command disables OSPF graceful restart.

- **Format**: `no nsf [ ietf ]`
- **Mode**: OSPFv3 Router Configuration mode

**nsf helper (OSPFv3)**

This command allows OSPF to act as a helpful neighbor for a restarting router. The `planned-only` parameter indicates that OSPF should only help a restarting router performing a planned restart.
The grace LSA announcing the graceful restart includes the reason for the restart. Reasons 1 (software restart) and 2 (software reload/upgrade) are considered planned restarts. Reasons 0 (unknown) and 3 (switch to redundant control processor) are considered unplanned restarts.

**Default**
OSPF acts as a helpful neighbor for both planned and unplanned restarts

**Format**
nsf helper [planned-only]

**Mode**
OSPFv3 Router Configuration mode

**nsf ietf helper disable (OSPFv3)**
This command is functionally equivalent to `no nsf helper` and is supported solely for IS-CLI compatibility.

**Format**
nsf ietf helper disable

**Mode**
OSPFv3 Router Configuration mode

**no nsf helper (OSPFv3)**
This command prevents OSPF from acting as a helpful neighbor.

**Format**
no nsf helper

**Mode**
OSPFv3 Router Configuration mode

**nsf helper strict-lsa-checking (OSPFv3)**
This command requires that an OSPF helpful neighbor exit helper mode when a topology change occurs. 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 might introduce forwarding loops or black holes that persist until the graceful restart is completed. By exiting graceful restart when a topology change occurs, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router.

The `ietf` parameter is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is not the only one supported, this parameter is optional.

A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

**Default**
A helpful neighbor exits helper mode when a topology change occurs.

**Format**
nsf [ietf] helper strict-lsa-checking

**Mode**
OSPFv3 Router Configuration mode
**no nsf [ietf] helper strict-lsa-checking (OSPFv3)**

This command allows OSPF to continue as a helpful neighbor in spite of topology changes.

**nsf restart-interval (OSPFv3)**

This command configures the length of the grace period on the restarting router. 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 its neighbors.

The *ietf* parameter is used to distinguish the IETF standard implementation of graceful restart from other implementations. Since the IETF implementation is not the only one supported, this parameter is optional. The *seconds* parameter represents the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The restarting router includes the restart interval in its grace LSAs (range 1–1800 seconds).

**Default**

120s

**Format**

nsf [ietf] restart-interval seconds

**Mode**

OSPFv3 Router Configuration mode

**no [ietf] nsf restart-interval (OSPFv3)**

This command reverts the grace period to its default.

**DHCPv6 Commands**

This section describes the command you use to configure the DHCPv6 server on the system and to view DHCPv6 information.

**service dhcpv6**

This command enables DHCPv6 configuration on the router.

**Default**

disabled

**Format**

service dhcpv6

**Mode**

Global Config

**no service dhcpv6**

This command disables DHCPv6 configuration on router.

**Format**

no service dhcpv6

**Mode**

Global Config
**IPv6 Commands**

**ipv6 dhcp server**

Use this command to configure DHCPv6 server functionality on an interface. The `<pool-name>` is the DHCPv6 pool containing stateless and/or prefix delegation parameters, `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> [rapid-commit] [preference <pref-value>]
```

**Mode**

Interface Config

**ipv6 dhcp relay destination**

Use this command to configure an interface for DHCPv6 relay functionality. 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 (unit/slot/port) to reach a relay server. The optional `remote-id` is the Relay Agent Information Option “remote ID” sub-option 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.

**Note:** 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>}] | interface [<relay-interface>]} [remote-id (duid-ifid | <user-defined-string>)]
```

**Mode**

Interface Config

**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 alpha-numeric 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.

**Format**
```
ipv6 dhcp pool <pool-name>
```

**Mode**
Global Config

**no ipv6 dhcp pool**

This command removes the specified DHCPv6 pool.

**Format**
```
no ipv6 dhcp pool <pool-name>
```

**Mode**
Global Config

**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

**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

**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 maximum of 8.

**Format**
```
dns-server <dns-server-address>
```

**Mode**
IPv6 DHCP Pool Config

**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
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 <0-4294967295>] [preferred-lifetime < 0-4294967295>]

Mode
IPv6 DHCP Pool Config

no prefix-delegation

This command deletes a specific prefix-delegation client.

Format
no prefix-delegation <prefix/prefix-delegation> <DUID>

Mode
IPv6 DHCP Pool Config

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 (Disabled)</td>
<td>The status of the DHCPv6 server.</td>
</tr>
<tr>
<td>Server DUID</td>
<td>If configured, shows the DHCPv6 unique identifier.</td>
</tr>
</tbody>
</table>

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>
show ipv6 dhcp interface

This command displays DHCPv6 information for all relevant interfaces or the specified interface. If you specify an interface, you can use the optional `statistics` parameter to view statistics for the specified interface.

**Format**

```
show ipv6 dhcp interface <unit/slot/port> [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 <code>&lt;unit/slot/port&gt;</code> 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 <code>&lt;unit/slot/port&gt;</code> 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 412 for information about the output.

`clear ipv6 dhcp`

Use this command to clear DHCPv6 statistics for all interfaces or for a specific interface. Use the `<unit/slot/port>` parameter to specify the interface.

**Format**

```
clear ipv6 dhcp {statistics | interface <unit/slot/port> statistics}
```

**Mode**

Privileged EXEC
**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>

**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>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>Valid Lifetime</td>
<td>Valid lifetime in seconds for delegated prefix.</td>
</tr>
<tr>
<td>Preferred</td>
<td>Preferred lifetime in seconds for delegated prefix.</td>
</tr>
<tr>
<td>Lifetime</td>
<td></td>
</tr>
</tbody>
</table>
This chapter describes the IPv6 multicast commands available in the managed switch CLI.

**Note:** Commands described in this chapter that require a license are:
- IPv6 Multicast Forwarder Commands
- IPv6 PIM Commands
- IPv6 MLD Commands
- IPv6 MLD-Proxy Commands

This chapter contains the following sections:
- IPv6 Multicast Forwarder Commands on page 418
- IPv6 PIM Commands on page 420
- IPv6 MLD Commands on page 428
- IPv6 MLD-Proxy Commands on page 434

The commands in this chapter are in 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.

**Note:** There is no specific IP multicast enable for IPv6. Enabling of multicast at global config is common for both IPv4 and IPv6.
IPv6 Multicast Forwarder Commands

**Note:** There is no specific IP multicast enable for IPv6. Enabling of multicast at global config is common for both IPv4 and IPv6.

### 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 mcast e mroute` command.)

**Format**

```
show ipv6 mroute {detail | 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</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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>
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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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>

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> {detail | summary}

Modes  
• Privileged EXEC
• User EXEC

If you use the detail 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</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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</td>
<td>The IP address of the multicast data source.</td>
</tr>
<tr>
<td>Group IP</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>

### IPv6 PIM Commands

This section describes the Protocol Independent Multicast (PIM) commands that support the PIM version of IPv6.

**ipv6 pim dense (Global Config)**

Use this command to administratively enable PIM-DM Multicast Routing Mode across the router (Global Config).

- **Default**: disabled
- **Format**: `ipv6 pim dense`
- **Mode**: • Global Config • Interface Config

**no ipv6 pim dense (Global Config)**

Use this command to administratively disable PIM-DM Multicast Routing Mode either across the router (Global Config) or on a particular router (Interface Config).

- **Format**: `no ipv6 pim dense`
- **Mode**: Global Config

**ipv6 pim (Interface Config)**

Use this command to set the administrative mode of PIM on an interface to enabled.

- **Default**: disabled
- **Format**: `ipv6 pim`
- **Mode**: Interface Config
no ipv6 pim (Interface Config)

Use this command to set the administrative mode of PIM on an interface to disabled.

**Format**
no ipv6 pim

**Mode**
Interface Config

IPv6 pim hello-interval

Use this command to configure the PIM hello interval for the specified router interface. The hello-interval is specified in seconds and is in the range 10–18000.

**Default**
30

**Format**
ipv6 pim hello-interval <10-18000>

**Mode**
Interface Config

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

show ipv6 pim

Use this command to display PIM Global Configuration parameters and PIM interface status.

**Format**
show ipv6 pim

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM Mode</td>
<td>Configured mode of PIM protocol</td>
</tr>
<tr>
<td>Data Threshold Rate</td>
<td>Rate (in kbps) of SPT Threshold</td>
</tr>
<tr>
<td>Register Rate-limit</td>
<td>Rate (in kbps) of Register Threshold</td>
</tr>
<tr>
<td>Interface</td>
<td>Valid unit, slot, and port number separated by forward slashes</td>
</tr>
<tr>
<td>Interface-Mode</td>
<td>Indicates whether PIM-DM is enabled or disabled on this interface</td>
</tr>
<tr>
<td>Operational-Status</td>
<td>The current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.</td>
</tr>
</tbody>
</table>

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

(Switch) #show ipv6 pim
IPv6 Multicast Commands

ProSafe Managed Switch

PIM Mode..................................... Dense
Data Threshold Rate (Kbps)............... 0
Register Rate-limit (Kbps)............... 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface Mode</th>
<th>Operational-Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0/1</td>
<td>Enabled</td>
<td>Non-Operational</td>
</tr>
</tbody>
</table>

show ipv6 pim neighbor

Use this command to display the PIM neighbor information for all interfaces or for the specified interface.

Format          show ipv6 pim neighbor [<unit/slot/port>|vlan]
Modes
• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>The IP address of the neighbor on an interface.</td>
</tr>
<tr>
<td>Address</td>
<td></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>The expiry time of the neighbor on this interface.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>DR Priority configured on this interface (PM-SM only).</td>
</tr>
</tbody>
</table>

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

(Switch) #show ipv6 pim neighbor 0/1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Neighbor</th>
<th>Up Time</th>
<th>Expiry Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>(hh:mm:ss)</td>
<td>(hh:mm:ss)</td>
<td></td>
</tr>
</tbody>
</table>

show ipv6 pim interface

Use this command to display PIM configuration information for all interfaces or for the specified interface. If no interface is specified, configuration of all interfaces is displayed.

Format          show ipv6 pim interface [<unit/slot/port>|vlan]
Modes
• Privileged EXEC
• User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Active PIM protocol.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface number.</td>
</tr>
</tbody>
</table>
ProSafe Managed Switch

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Interval</td>
<td>Hello interval value. 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>Join-prune interval value.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>DR priority configured on this interface. This is not applicable if the interface mode is Dense.</td>
</tr>
<tr>
<td>BSR Border</td>
<td>Indicates whether the interface is configured as a BSR border.</td>
</tr>
<tr>
<td>Neighbor Count</td>
<td>Number of PIM neighbors discovered on the interface. This field is displayed only when the interface is operational.</td>
</tr>
<tr>
<td>Designated-Router</td>
<td>IP address of the elected DR on the interface. This field is displayed only when the interface is operational.</td>
</tr>
</tbody>
</table>

(Switch) #show ipv6 pim interface 1/0/1

Interface...................................... 1/0/1
Mode........................................... Dense
Hello Interval (secs).......................... 30
Join Prune Interval (secs)..................... 60
DR Priority.................................... 1
BSR Border..................................... Disabled

**ipv6 pim bsr-border**

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

Default  disabled
Format    ipv6 pim bsr-border
Mode      Interface Config

**no ipv6 pim bsr-border**

Use this command to disable the interface from being the BSR border.

Format    no ipv6 pim bsr-border
Mode      Interface Config

**ipv6 pim bsr-candidate**

Use this command to configure the router to announce its candidacy as a bootstrap router (BSR).

Default  None
IPv6 PIM Commands

**ipv6 pim bsr-candidate interface <unit/slot/port> [hash-mask-length] [priority]**

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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 IP address is the BSR. The default value is 0.</td>
</tr>
</tbody>
</table>

**no ipv6 pim bsr-candidate**

Use this command to disable the router to announce its candidacy as a bootstrap router (BSR).

**Format**

```
no ipv6 pim bsr-candidate interface <unit/slot/port> [hash-mask-length] [priority]
```

**Mode**
Global Config

**ipv6 pim dr-priority**

Use this command to set the priority value for which a router is elected as the designated router (DR).

**Default**

1

**Format**

```
ipv6 pim dr-priority <0-2147483647>
```

**Mode**
Interface Config

**no ipv6 pim dr-priority**

Use this command to disable the interface from being the BSR border.

**Format**

```
no ipv6 pim dr-priority
```

**Mode**
Interface Config
**ipv6 pim join-prune-interval**

Use this command to configure the interface join/prune interval for the PIM-SM router. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

Default: 60

Format: `ipv6 pim join-prune-interval <0-18000>`

Mode: Interface Config

**no ipv6 pim join-prune-interval**

Use this command to set the join/prune interval to the default value.

Format: `no ipv6 pim join-prune-interval`

Mode: Interface Config

**ipv6 pim register-rate-limit**

Use this command to configure the Register Threshold rate for the Rendezvous Point router to switch to a source-specific shortest path. The valid values are from (0 to 2000 kilobits/sec).

Default: 0

Format: `ipv6 pim register-rate-limit <0-2000>`

Mode: Global Config

**no ipv6 pim register-rate-limit**

Use this command to reset the register threshold rate for the Rendezvous Pointer router to the default value.

Format: `no ipv6 pim register-rate-limit`

Mode: Global Config

**ipv6 pim rp-address**

Use this command to statically configure the RP address for one or more multicast groups. The parameter `<rp-address>` is the IP address of the RP. The parameter `<groupaddress>` is the group address supported by the RP. The parameter `<groupmask>` is the group mask for the group address. The optional keyword `override` indicates that if
there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Default
Format ipv6 pim rp-address <rp-address> <group-address> <group-mask> [override]
Mode Global Config

no ipv6 pim rp-address

Use this command to statically remove the RP address for one or more multicast groups.

Format no ipv6 pim rp-address <rp-address> <group-address> <group-mask>
Mode Global Config

ipv6 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).

Default None
Format ipv6 pim rp-candidate interface <unit/slot/port> <group-address> <group-mask>
Mode Global Config

no ipv6 pim rp-candidate

Use this command 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 <unit/slot/port> <group-address> <group-mask>
Mode Global Config

ipv6 pim spt-threshold

Use this command to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The rate is specified in Kilobits per second. The possible values are 0 to 2000.

Default 0
Format ipv6 pim spt-threshold <1-2000>
Mode Global Config
**no ipv6 pim spt-threshold**

This command is used to set the Data Threshold rate for the RP router to the default value.

**Format**
```
no ipv6 pim spt-threshold
```

**Mode**
Global Config

**ipv6 pim ssm**

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

**Default**
`disabled`

**Format**
```
ipv6 pim ssm {default | <group-address/prefixlength> <group-mask>}
```

**Mode**
Global Config

**Parameter** | **Description**
---|---
Default | Defines the SSM range access list to 232/8.

**no ipv6 pim ssm**

Use this command to disable the Source Specific Multicast (SSM) range.

**Format**
```
no ipv6 pim ssm
```

**Mode**
Global Config

**show ipv6 pim bsr-router**

Use command to display the bootstrap router (BSR) information. The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

**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>IP address of the BSR.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Length of time that this router has been up (in hours, minutes, and seconds).</td>
</tr>
<tr>
<td>BSR Priority</td>
<td>Priority as configured in the <code>ip pim bsr-candidate</code> command.</td>
</tr>
<tr>
<td>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 <code>ip pim bsr-candidate</code> command.</td>
</tr>
</tbody>
</table>
IPv6 Multicast Commands

Use this command to display 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>Next Bootstrap Message In</td>
<td>Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.</td>
</tr>
<tr>
<td>Next Candidate RP advertisement in</td>
<td>Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.</td>
</tr>
<tr>
<td>RP</td>
<td>The IP address of the RP for the group specified.</td>
</tr>
<tr>
<td>Origin</td>
<td>Indicates the mechanism (BSR or static) by which the RP was selected.</td>
</tr>
</tbody>
</table>

**show ipv6 pim rp mapping**

Use this command to display all group-to-RP mappings of which the router is aware (either configured or learned from the bootstrap router (BSR)). If no RP is specified, all active RPs are displayed.

**Format**

```
show ipv6 pim rp mapping [rp address]
```

**Modes**

- Privileged EXEC
- User EXEC

**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, the 7000 series 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 161 and [MLD Snooping Commands](#) on page 172.
**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
  • Interface Config

**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
  • Interface Config

**ipv6 mld query-interval**

Use this command to set the MLD router’s query interval for the interface. 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

**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

**ipv6 mld query-max-response-time**

Use this command to set the MLD querier’s maximum response time for the interface 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
**IPv6 Multicast Commands**

**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
```

**ipv6 mld last-member-query-interval**

Use this command to set the last member query interval for the MLD interface, 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 1 to 65535 milliseconds.

```
Default  1000 milliseconds
Format    ipv6 mld last-member-query-interval  <last-member-query-interval>
Mode       Interface Config
```

**no ipv6 mld last-member-query-interval**

Use this command to reset the `<last-member-query-interval>` parameter of the interface to the default value.

```
Format    no ipv6 mld last-member-query-interval
Mode       Interface Config
```

**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 the interface. The range for `<last-member-query-count>` is 1 to 20.

```
Default   2
Format     ipv6 mld last-member-query-count  <last-member-query-count>
Mode       Interface Config
```
no ipv6 mld last-member-query-count

Use this command to reset the `<last-member-query-count>` parameter of the interface to the default value.

Format: `no ipv6 mld last-member-query-count`

Mode: Interface Config

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.

Format: `show ipv6 mld groups {<unit/slot/port> | <group-address>}`

Mode:
- Privileged EXEC
- User EXEC

The following fields are displayed as a table when `<unit/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 <code>include</code> and <code>exclude</code>.</td>
</tr>
<tr>
<td>Version 1 Host Timer</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 <code>MLDv1</code> and <code>MLDv2</code>.</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.

(Switch) #show ipv6 mld groups ?
<group-address> Enter Group Address Info.
<unit/slot/port> Enter interface in unit/slot/port format.

(Switch) #show ipv6 mld groups 1/0/1
Group Address................................. FF43::3
Interface.................................... 1/0/1
Up Time (hh:mm:ss)............................ 00:03:04
Expiry Time (hh:mm:ss)....................... -----

(Switch) #show ipv6 mld groups ff43::3
Interface.................................... 1/0/1
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

<table>
<thead>
<tr>
<th>Source Address</th>
<th>ExpiryTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003::10</td>
<td>00:04:17</td>
</tr>
<tr>
<td>2003::20</td>
<td>00:04:17</td>
</tr>
</tbody>
</table>

**show ipv6 mld interface**

Use this command to display MLD-related information for the interface.

**Format**

show ipv6 mld interface [<unit/slot/port>]

**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 unit/slot/port format.</td>
</tr>
<tr>
<td>MLD Global Mode</td>
<td>Displays the configured administrative status of MLD.</td>
</tr>
<tr>
<td>MLD 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>Query Max Response Time</td>
<td>Indicates the configured maximum query response time (in seconds) advertised in MLD queries on this 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>
</tbody>
</table>
IPv6 Multicast Commands

ProSafe Managed Switch

**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.

<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>

**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

---

IPv6 Multicast Commands

434
**ipv6 mld-proxy**

Use this command to enable MLD-Proxy on the router. To enable MLD-Proxy on the router, 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

**no ipv6 mld-proxy**

Use this command to disable MLD-Proxy on the router.

**Format**

no ipv6 mld-proxy

**Mode**

Interface Config

**ipv6 mld-proxy unsolicit-rprt-interval**

Use this command to set the unsolicited report interval for the MLD-Proxy router. 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

**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

**ipv6 mld-proxy reset-status**

Use this command to reset the host interface status parameters of the MLD-Proxy router. This command is only valid when you enable MLD-Proxy on the interface.

**Format**

ipv6 mld-proxy reset-status

**Mode**

Interface Config
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>
<tr>
<td>Older Version 1 Querier Timeout</td>
<td>The interval used to timeout the older version 1 queriers.</td>
</tr>
<tr>
<td>Proxy Start Frequency</td>
<td>The number of times the MLD-Proxy has been stopped and started.</td>
</tr>
</tbody>
</table>

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

(Switch) #show ipv6 mld-proxy

Interface Index............................................. 1/0/3
Admin Mode................................................ Enable
Operational Mode........................................... Enable
Version......................................................... 3
Num of Multicast Groups......................... 0
Unsolicited Report Interval..................... 1
Querier IP Address on Proxy Interface........ fe80::1:2:5
Older Version 1 Querier Timeout.............. 00:00:00
Proxy Start Frequency..........................
**show ipv6 mld-proxy interface**

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Index</td>
<td>The unit/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.

```
(Switch) #show ipv6 mld-proxy interface

Interface Index................................. 1/0/1

Ver     Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
---------------------------------------------
1        2            0            0            0            2
2        3            0            4            -----        -----  
```

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

(Switch) #show ipv6 mld-proxy groups

<table>
<thead>
<tr>
<th>Interface Index</th>
<th>Interface</th>
<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>1/0/3</td>
<td>FF1E::1 FE80::100:2.3</td>
<td>00:01:40</td>
<td>DELAY_MEMBER</td>
<td>Exclude</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FF1E::2 FE80::100:2.3</td>
<td>00:02:40</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FF1E::3 FE80::100:2.3</td>
<td>00:01:40</td>
<td>DELAY_MEMBER</td>
<td>Exclude</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FF1E::4 FE80::100:2.3</td>
<td>00:02:44</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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>
</tbody>
</table>
IPv6 Multicast Commands

ProSafe Managed Switch

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>• <em>Idle Member</em>. The interface has responded to the latest group membership query for this group.</td>
</tr>
<tr>
<td></td>
<td>• <em>Delay Member</em>. 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 <em>Include</em> or <em>Exclude</em>.</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>The time left for a source to get deleted.</td>
</tr>
</tbody>
</table>

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

(Switch) #show ipv6 igmp-proxy groups

Interface Index......................... 1/0/3

<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>244</td>
<td>DELAY_MEMBER</td>
<td>Exclude</td>
<td>2</td>
</tr>
</tbody>
</table>

Group Source List
------------------
2001::1 00:02:40
2001::2 ----

Expiry Time
------------

<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::2</td>
<td>FE80::100:2.3</td>
<td>243</td>
<td>DELAY_MEMBER</td>
<td>Include</td>
<td>1</td>
</tr>
</tbody>
</table>

Group Source List
------------------
3001::1 00:03:32
3002::2 00:03:32

Expiry Time
------------

<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::3</td>
<td>FE80::100:2.3</td>
<td>328</td>
<td>DELAY_MEMBER</td>
<td>Exclude</td>
<td>0</td>
</tr>
</tbody>
</table>

Group Source List
------------------
4001::1 00:03:40
5002::2 00:03:40
4001::2 00:03:40
5002::2 00:03:40

Expiry Time
------------

IPv6 Multicast Commands

439
Quality of Service (QoS) Commands

This chapter describes the Quality of Service (QoS) commands available in the managed switch CLI.

This chapter contains the following sections:

- Class of Service (CoS) Commands
- Differentiated Services (DiffServ) Commands
- DiffServ Class Commands
- DiffServ Policy Commands
- DiffServ Service Commands
- DiffServ Show Commands
- MAC Access Control List (ACL) Commands
- IP Access Control List (ACL) Commands
- IPv6 Access Control List (ACL) Commands
- Time Range Commands for Time-Based ACLs
- Auto-Voice over IP Commands

The commands in this chapter are in 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.

Class of Service (CoS) Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.
Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

**classofservice dot1p-mapping**

This command maps an 802.1p priority to an internal traffic class. The `<userpriority>` values can range from 0-7. The `<trafficclass>` values range from 0-6, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see Voice VLAN Commands on page 79.

**Format**

```
classofservice dot1p-mapping <userpriority> <trafficclass>
```

**Modes**

- Global Config
- Interface Config

**no classofservice dot1p-mapping**

This command maps each 802.1p priority to its default internal traffic class value.

**Format**

```
noclassofservice dot1p-mapping
```

**Modes**

- Global Config
- Interface Config

**classofservice ip-dscp-mapping**

This command maps an IP DSCP value to an internal traffic class. The `<ipdscp>` value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

The `<trafficclass>` values can range from 0-6, although the actual number of available traffic classes depends on the platform.

**Format**

```
classofservice ip-dscp-mapping <ipdscp> <trafficclass>
```

**Modes**

- Global Config
- Interface Config

**no classofservice ip-dscp-mapping**

This command maps each IP DSCP value to its default internal traffic class value.

**Format**

```
noclassofservice ip-dscp-mapping
```

**Modes**

- Global Config
- Interface Config
ProSafe Managed Switch

**classofservice trust**

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the `show running config` command because Dot1p is the default.

**Note:** The classofservice trust dot1p command will not be supported in future releases of the software because Dot1p is the default value. Use the no classofservice trust command to set the mode to the default value.

<table>
<thead>
<tr>
<th>Default</th>
<th>dot1p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>`classofservice trust {dot1p</td>
</tr>
</tbody>
</table>
| Modes    | • Global Config  
          | • Interface Config |

**no classofservice trust**

This command sets the interface mode to the default value.

| Format   | `no classofservice trust` |
| Modes    | • Global Config  
          | • Interface Config |

**cos-queue min-bandwidth**

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The total number of queues supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

| Format   | `cos-queue min-bandwidth <bw-0> <bw-1> ... <bw-n>` |
| Modes    | • Global Config  
          | • Interface Config |
**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

**cos-queue strict**

This command activates the strict priority scheduler mode for each specified queue.

**Format**

```
cos-queue strict <queue-id-1> [<queue-id-2> ... <queue-id-n>]
```

**Modes**

- Global Config
- Interface Config

**no cos-queue strict**

This command restores the default weighted scheduler mode for each specified queue.

**Format**

```
no cos-queue strict <queue-id-1> [<queue-id-2> ... <queue-id-n>]
```

**Modes**

- Global Config
- Interface Config

**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 randomdetect queue-parms and the random-detect exponential-weighting-constant commands. 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 is platform dependant and corresponds to the number of supported queues (traffic classes).

**Format**

```
cos-queue random-detect queue-id-1 [queue-id-2 ... queue-id-n]
```

**Modes**

- Global Config
- Interface Config
**no cos-queue random-detect**

Use this command to disable WRED and restore the default tail drop operation for the specified queues on all interfaces or one interface.

**Format**

```
no cos-queue random-detect queue-id-1 [queue-id-2 ... queue-id-n]
```

**Modes**

- Global Config
- Interface Config

**random-detect exponential weighting-constant**

Use this command to configure the WRED decay exponent for a CoS queue interface.

**Format**

```
random-detect exponential-weighting-constant 0-15
```

**Modes**

- Global Config
- Interface Config

**Default**

`9`

**no random-detect exponential weighting-constant**

Use this command to reset the WRED decay exponent to the default value on all interfaces or one interface.

**Format**

```
no random-detect exponential-weighting-constant 0-15
```

**Modes**

- Global Config
- Interface Config

**random-detect queue-parms**

Use this command to configure WRED parameters for each drop precedence level supported by a queue. Use it only when per-COS queue configuration is enabled (using the `cos-queue random-detect` command).

`min-thresh` is the minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.

`max-thresh` is the maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.

`drop-probability` is 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). 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.

**Format**
```
random-detect queue-parms queue-id-1 [queue-id-2 ... queue-id-n]
minthresh thresh-prec-1 ... thresh-prec-n max-thresh thresh-prec-1 ...
threshprec-n drop-probability prob-prec-1 ... prob-prec-n
```

**Modes**
- Global Config
- Interface Config

**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

**traffic-shape**

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

**Format**
```
traffic-shape <bw>
```

**Modes**
- Global Config
- Interface Config

**no traffic-shape**

This command restores the interface shaping rate to the default value.

**Format**
```
no traffic-shape
```

**Modes**
- Global Config
- Interface Config

**show classofservice dot1p-mapping**

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The `<unit/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 79.

**Format**
```
show classofservice dot1p-mapping [<unit/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>

**show classofservice ip-precedence-mapping**

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The unit/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 [<unit/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>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>

**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>

**show classofservice trust**

This command displays the current trust mode setting for a specific interface. The `<unit/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 [<unit/slot/port>]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-IP Traffic Class</td>
<td>The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).</td>
</tr>
<tr>
<td>Untrusted Traffic Class</td>
<td>The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.</td>
</tr>
</tbody>
</table>

**show interfaces cos-queue**

This command displays the class-of-service queue configuration for the specified interface. The unit/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 [<unit/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>Minimum Bandwidth</td>
<td>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.</td>
</tr>
<tr>
<td>Scheduler Type</td>
<td>Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.</td>
</tr>
<tr>
<td>Queue Management Type</td>
<td>The queue depth management technique used for this queue (tail drop).</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The unit/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>
</tbody>
</table>
Differentiated Services (DiffServ) Commands

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

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

1. Class
   a. Creating and deleting classes.
   b. Defining match criteria for a class.

2. Policy
   a. Creating and deleting policies
   b. Associating classes with a policy
   c. Defining policy statements for a policy/class combination

3. Service
   a. Adding and removing a policy to/from an inbound or outbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

• Each class can contain a maximum of one referenced (nested) class
• Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

Note: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.
**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

**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

---

**DiffServ Class Commands**

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria).

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

---

**Note:** Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

---

The CLI command root is **class-map**.

**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.

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 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.

```plaintext
Format: class-map match-all <class-map-name> [{ipv4 | ipv6}]
Mode: Global Config
```

`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.

```plaintext
Format: no class-map <class-map-name>
Mode: Global Config
```

`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.

```plaintext
Default: none
Format: class-map rename <class-map-name> <new-class-map-name>
Mode: Global Config
```
**match ethertype**

This command adds to the specified class definition a match condition based on the value of the ethertype. The `<ethertype>` value is specified as one of the following keywords: `appletalk`, `arp`, `ibmsna`, `ipv4`, `ipv6`, `ipx`, `mplsmcast`, `mplsucast`, `netbios`, `novell`, `pppoe`, `rarp` or as a custom ethertype value in the range of 0x0600-0xFFFF.

**Format**

```
match ethertype {<keyword> | custom <0x0600-0xFFFF>}
```

**Mode**

Class-Map Config  
Ipv6-Class-Map Config

**match any**

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

**Default**

`none`

**Format**

```
match any
```

**Mode**

Class-Map Config  
Ipv6-Class-Map Config

**match class-map**

This command adds to the specified class definition the set of match conditions defined for another class. The `<refclassname>` is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

**Default**

`none`

**Format**

```
match class-map <refclassname>
```

**Mode**

Class-Map Config  
Ipv6-Class-Map Config

Note the following:

- 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 reclass rule reduces the maximum number of available rules in the class definition by one.
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

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.

Default: none
Format: match cos <0-7>
Mode: Class-Map Config

match secondary cos

This command adds to the specified class definition a match condition for the secondary 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.

Default: none
Format: match secondary-cos <0-7>
Mode: Class-Map Config

match ip6flowlbl

This command adds to the specified class definition a match condition based on the IP6flowlbl of a packet. The label is the value to match in the Flow Label field of the IPv6 header (range 0-1048575).

Format: match ip6flowlbl <label>
Mode: Ipv6-Class-Map Configuration mode

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).

**Default**
none

**Format**
match destination-address mac `<macaddr> <macmask>`

**Mode**
Class-Map Config
Ipv6-Class-Map Config

**match dstip**

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The `<ipaddr>` parameter specifies an IP address. The `<ipmask>` parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

**Default**
none

**Format**
match dstip `<ipaddr> <ipmask>`

**Mode**
Class-Map Config

**match dstip6**

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

**Default**
none

**Format**
match dstip6 `<destination-ipv6-prefix/prefix-length>`

**Mode**
Ipv6-Class-Map Config

**match dstl4port**

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for `<portkey>` is one of the supported port name keywords. The currently supported `<portkey>` values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535.

**Default**
none

**Format**
match dstl4port `{<portkey> | <0-65535>}`

**Mode**
Class-Map Config
Ipv6-Class-Map Config
**match ip dscp**

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The `<dscpval>` value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

**Note:** The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

**Default**  none

**Format**  match ip dscp  `<dscpval>`

**Mode**  Class-Map Config  Ipv6-Class-Map Config

**match ip precedence**

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7.

**Note:** The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

**Default**  none

**Format**  match ip precedence  `<0-7>`

**Mode**  Class-Map Config

**match ip tos**

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of `<tosbits>` is a two-digit hexadecimal number from 00 to ff. The
value of `<tosmask>` is a two-digit hexadecimal number from 00 to ff. The `<tosmask>`
denotes the bit positions in `<tosbits>` that are used for comparison against the IP TOS
field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1
clear, where bit 7 is most significant, use a `<tosbits>` value of a0 (hex) and a `<tosmask>`
of a2 (hex).

**Note:** The IP DSCP, IP Precedence, and IP ToS match conditions are
alternative ways to specify a match criterion for the same Service
Type field in the IP header, but with a slightly different user notation.

**Note:** This “free form” version of the IP DSCP/Precedence/TOS match
specification gives the user complete control when specifying which
bits of the IP Service Type field are checked.

Default: none
Format: `match ip tos <tosbits> <tosmask>`
Mode: Class-Map Config

**match protocol**

This command adds to the specified class definition a match condition based on the value of
the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for
`<protocol-name>` is one of the supported protocol name keywords. The currently
supported values are: `icmp`, `igmp`, `ip`, `tcp`, `udp`. A value of `ip` matches all protocol number
values.

To specify the match condition using a numeric value notation, the protocol number is a
standard value assigned by IANA and is interpreted as an integer from 0 to 255.

**Note:** This command does not validate the protocol number value against
the current list defined by IANA.
ProSafe Managed Switch

**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).

**Default**

```none```

**Format**

`match source-address mac <address> <macmask>`

**Mode**

Class-Map Config

Ipv6-Class-Map Config

**match srcip**

This command adds to the specified class definition a match condition based on the source IP address of a packet. The `<ipaddr>` parameter specifies an IP address. The `<ipmask>` parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

**Default**

```none```

**Format**

`match srcip <ipaddr> <ipmask>`

**Mode**

Class-Map Config

**match srcip6**

This command adds to the specified class definition a match condition based on the source IP address of a packet.

**Default**

```none```

**Format**

`match srcip6 <source-ipv6-prefix/prefix-length>`

**Mode**

Ipv6-Class-Map Config

**match src14port**

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,
Quality of Service (QoS) Commands

ProSafe Managed Switch

echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535.

**Default** none

**Format** `match srcl4port {<portkey> | <0-65535>}`

**Mode** Class-Map Config

**ipv6-Class-Map Config**

**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 802.1Q tag of a VLAN tagged packet). The VLAN is an integer from 0 to 4095.

**Default** none

**Format** `match vlan {<0-4095>}`

**Mode** Class-Map Config

**ipv6-Class-Map Config**

**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 802.1Q tag of a double VLAN tagged packet). The VLAN is an integer from 0 to 4095.

**Default** none

**Format** `match secondary-vlan {<0-4095>}`

**Mode** Class-Map Config

**ipv6-Class-Map Config**

**DiffServ Policy Commands**

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes.

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the
conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

---

**Note:** The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

---

The CLI command root is `policy-map`.

**assign-queue**

This command modifies the queue id to which the associated traffic stream is assigned. The `queueid` is an integer from 0 to \( n-1 \), where \( n \) is the number of egress queues supported by the device.

**Format**

```
assign-queue <queueid>
```

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop

**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

**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 <unit/slot/port>
```

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Redirect
**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 <unit/slot/port>`

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Mirror

**conform-color**

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The `<class-map-name>` parameter is the name of an existing DiffServ class map.

---

**Note:** This command may only be used after specifying a police command for the policy-class instance.

---

**Format**

`conform-color <class-map-name>`

**Mode**

Policy-Class-Map Config

**class**

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The `<classname>` is the name of an existing DiffServ class.

---

**Note:** This command causes the specified policy to create a reference to the class definition.

---

**Note:** The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

---

**Format**

`class <classname>`

**Mode**

Policy-Map Config
**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.

---

**Note:** This command removes the reference to the class definition for the specified policy.

---

**Format**

```yaml
no class <classname>
```

**Mode**

Policy-Map Config

**mark cos**

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

**Default**

1

**Format**

```yaml
mark-cos <0-7>
```

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Mark IP DSCP, IP Precedence, Police

**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**

```yaml
mark-cos-as-sec-cos
```

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Mark IP DSCP, IP Precedence, Police

**mark ip-dscp**

This command marks all packets for the associated traffic stream with the specified IP DSCP value.
The `<dscpval>` value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

**Format**

`mark ip-dscp <dscpval>`

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Mark CoS, Mark IP Precedence, Police

### mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

**Format**

`mark ip-precedence <0-7>`

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Mark CoS, Mark IP Precedence, Police

**Policy Type**

In

### police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop.

For set-dscp-transmit, a `<dscpval>` value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.
For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

**Format**

```
policy-simple {(<1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit}) [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit}]
```

**Mode**

Policy-Class-Map Config

**Incompatibilities**

Drop, Mark (all forms)

---

**police-two-rate**

This command is the two-rate form of the `police` 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-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the `police` 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

---

**policy-map**

This command establishes a new DiffServ policy. The `<policyname>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the `in` parameter.

---

**Note:** The CLI mode is changed to Policy-Map Config when this command is successfully executed.

**Format**

```
policy-map <policyname> [in|out]
```

**Mode**

Global Config
no policy-map

This command eliminates an existing DiffServ policy. The \(<\text{policyname}>\) 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 \(<\text{policyname}>\)
Mode    Global Config

policy-map rename

This command changes the name of a DiffServ policy. The \(<\text{policyname}>\) is the name of an existing DiffServ class. The \(<\text{newpolicyname}>\) parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format  policy-map rename \(<\text{policyname}>\) \(<\text{newpolicyname}>\)
Mode    Global Config

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.

service-policy

This command attaches a policy to an interface in the inbound direction. The \(<\text{policyname}>\) parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

\[\textbf{Note:}\] This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.
**Note:** This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

**Format**  
```
no service-policy in <policyname>
```

**Modes**  
- Global Config
- Interface Config

**Note:** Each interface can have one policy attached.

**no service-policy**

This command detaches a policy from an interface in the inbound direction. The `<policyname>` parameter is the name of an existing DiffServ policy.

**Note:** This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

**Format**  
```
no service-policy in <policyname>
```

**Modes**  
- Global Config
- Interface Config

**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.
show class-map

This command displays all configuration information for the specified class. The `<class-name>` is the name of an existing DiffServ class.

**Format**

```
show class-map <class-name>
```

**Modes**

- Privileged EXEC
- User EXEC

If the class-name is specified the following fields are displayed:

<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>
<tr>
<td>Match Criteria</td>
<td>The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.</td>
</tr>
<tr>
<td>Values</td>
<td>The values of the Match Criteria.</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>Reference 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>

**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
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>
</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>
</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>
**show diffserv service**

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

**Format**

```
show diffserv service <unit/slot/port> [in | out]
```

**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>Valid slot and port number separated by forward slashes.</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 <code>&lt;policymapname&gt;</code> command (content not repeated here for brevity).</td>
</tr>
</tbody>
</table>

**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 | out]
```

**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 active on an interface while DiffServ is in an enabled mode.</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>Valid slot and port number separated by forward slashes.</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>
**show policy-map interface**

This command displays policy-oriented statistics information for the specified interface and direction. The `<unit/slot/port>` parameter specifies a valid interface for the system.

**Note:** This command is only allowed while the DiffServ administrative mode is enabled.

| Format | show policy-map interface <unit/slot/port> [in | out] |
|--------|------------------------------------------------------|
| Mode   | Privileged EXEC                                      |

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Valid slot and port number separated by forward slashes.</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>
</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>Class Name</td>
<td>The name of this class instance.</td>
</tr>
<tr>
<td>In Discarded</td>
<td>A count of the packets discarded for this class instance for any reason</td>
</tr>
<tr>
<td>Packets</td>
<td>due to DiffServ treatment of the traffic class.</td>
</tr>
</tbody>
</table>

**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|out} |
|--------|-------------------------------|
| 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>Valid slot and port number separated by forward slashes.</td>
</tr>
</tbody>
</table>
This section describes the commands you use to configure MAC ACL settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.

`mac access-list extended`  
This command creates a MAC Access Control List (ACL) identified by `<name>`, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The `<name>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

**Note:** The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

```
Format     mac access-list extended <name>
Mode       Global Config
```

`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
```
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

{deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

---

**Note:** The 'no' form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and re-specified.

---

**Note:** An implicit 'deny all' MAC rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported `<ethertypekey>` values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplscast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

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.

<table>
<thead>
<tr>
<th>Ethertype Keyword</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>0x86DD</td>
</tr>
<tr>
<td>ipx</td>
<td>0x8037</td>
</tr>
<tr>
<td>mpls-mcast</td>
<td>0x8848</td>
</tr>
<tr>
<td>mpls-ucast</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 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.

**Note:** The special command form {deny | permit} any any is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

**Format**

{deny|permit} {<srcmac> | any} {<dstmac> | any} [ethertypekey | <0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [log] [time-range <time-range-name>] [assign-queue <queue-id>] [(mirror | redirect) <unit/slot/port>]

**Mode**

Mac-Access-List Config
**mac access-group**

This command either attaches a specific MAC Access Control List (ACL) identified by `<name>` to an interface, or associates it with a VLAN ID, in a given direction. The `<name>` parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

**Note:** The `<out>` option may or may not be available, depending on the platform.

**Format**

```
mac access-group <name> [vlan <vlan-id>] [in|out] [sequence <1-4294967295>]
```

**Modes**

- Global Config
- Interface Config

**no mac access-group**

This command removes a MAC ACL identified by `<name>` from the interface in a given direction.

**Format**

```
no mac access-group <name> [vlan <vlan-id>] in
```

**Modes**

- Global Config
- Interface Config

**show mac access-lists**

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the `[name]` parameter to identify a specific MAC ACL to display.

**Format**

```
show mac access-lists [name]
```

**Mode**

Privileged EXEC
IP Access Control List (ACL) Commands

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

The following rules apply to IP ACLs:

- Managed switch 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.
- 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.
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.

**IP Standard ACL:**

**Format**
```
access-list <1-99> {deny | permit} {every | <srcip> <srcmask>} [log]
[assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>]
```

**Mode**
Global Config

**IP Extended ACL:**

**Format**
```
access-list <100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask> [{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq {<portkey> | <0-65535>}]}] [precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>]
```

**Mode**
Global Config

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-99&gt; or &lt;100-199&gt;</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>{deny</td>
<td>permit}</td>
</tr>
<tr>
<td>every</td>
<td>Match every packet</td>
</tr>
<tr>
<td>{icmp</td>
<td>igmp</td>
</tr>
<tr>
<td>&lt;srcip&gt; &lt;srcmask&gt;</td>
<td>Specifies a source IP address and source netmask for match condition of the IP ACL rule.</td>
</tr>
<tr>
<td>[{eq {&lt;portkey&gt;</td>
<td>&lt;0-65535&gt;}}]</td>
</tr>
<tr>
<td>&lt;dstip&gt; &lt;dstmask&gt;</td>
<td>Specifies a destination IP address and netmask for match condition of the IP ACL rule.</td>
</tr>
<tr>
<td>[precedence &lt;precedence&gt;</td>
<td>tos &lt;tos&gt; &lt;tosmask&gt;</td>
</tr>
<tr>
<td>[log]</td>
<td>Specifies that this rule is to be logged.</td>
</tr>
</tbody>
</table>
### 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**

```plaintext
no access-list <accesslistnumber>
```

**Mode**
Global Config

### ip access-list

This command creates an extended IP Access Control List (ACL) identified by `<name>`, consisting of classification fields defined for the IP header of an IPv4 frame. The `<name>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

---

**Note:** The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

---

The time-range parameter 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 IP 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 IP 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.

**IP Standard ACL:**

**Format**

```plaintext
ip access-list access-list <1-99> {deny | permit} {every | <srcip> <srcmask>} [log] [time-range <timerange-name>] [assignqueue <queue-id>] [[mirror | redirect] <unit/slot/port>]
```

**Mode**
Global Config

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[assign-queue &lt;queue-id&gt;]</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] &lt;unit/slot/port&gt;]</td>
</tr>
</tbody>
</table>

---
IP Extended ACL:

Format
access-list <100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} <srcip> <srcmask>
{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq {<portkey> | <0-65535>}
[precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>]} [log] [time-range <time-range-name>] [assign-queue <queue-id>]
[<mirror | redirect} <unit/slot/port>]

Mode
Global Config

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

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 is an IP ACL by the name <newname> already exists.

Format
ip access-list rename <name> <newname>

Mode
Global Config

{deny | permit} (IP ACL)

This command creates a new rule for the current IP access list. Each rule is appended to the
list of configured rules for the list.

Note: The “no” form of this command is not supported, since the rules
within an IP ACL cannot be deleted individually. Rather, the entire IP
ACL must be deleted and re-specified.

Note: An implicit “deny all” IP rule always terminates the access list.
**Note:** For the XSM7224S, 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.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified using the keyword 'any' to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed `<queue-id>` value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The `assign-queue` parameter is valid only for a permit rule.

The `time-range` parameter allows imposing time limitation on the IP ACL rule as defined by the parameter `<time-range-name>`. If a time range with the specified name does not exist and the IP 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 IP 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.

**Format**
```
{deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>}
<srcip> <srcmask>[{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq
<{portkey}> | <0-65535>]} [precedence <precedence> | tos <tos>
<tosmask> | dscp <dscp>] [log] [timerange <time-range-name>]
[assign-queue <queue-id>] [{mirror | redirect}
<unit/slot/port>]
```

**Mode**
```
IpV4-Access-List Config
```

**ip access-group**

This command either attaches a specific IP ACL identified by `<accesslistnumber>` to an interface or associates with a VLAN ID in a given direction. The parameter `<name>` is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a
sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

**Note:** You should be aware that the `<out>` option may or may not be available, depending on the platform.

---

**Default**

- none

**Format**

```
ip access-group {<accesslistnumber>|<name>} [vlan <vlan-id>] <in | out>[sequence <1-4294967295>]
```

**Modes**

- Interface Config
- Global Config

**no ip access-group**

This command removes a specified IP ACL from an interface.

**Default**

- none

**Format**

```
no ip access-group <accesslistnumber> [vlan <vlan-id>] in
```

**Mode**

- Interface Config
- Global Config

**acl-trapflags**

This command enables the ACL trap mode.

**Default**

- disabled

**Format**

```
acl-trapflags
```

**Mode**

- Global Config

**no acl-trapflags**

This command disables the ACL trap mode.

**Format**

```
no acl-trapflags
```

**Mode**

- Global Config
**show ip access-lists**

This command displays an IP ACL `<accesslistnumber>` is the number used to identify the IP ACL.

**Format**  
`show ip access-lists <accesslistnumber>`

**Mode**  
Privileged EXEC

---

**Note:** Only the access list fields that you configure are displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 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>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>
<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>
</tbody>
</table>
show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction.

**Format**

```
show access-lists interface <unit/slot/port> [in|out]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range Name</td>
<td>Displays the name of the time-range if the ACL rule has referenced a time range.</td>
</tr>
<tr>
<td>Rule Status</td>
<td>Status (Active/Inactive) of the ACL rule.</td>
</tr>
</tbody>
</table>

**IPv6 Access Control List (ACL) Commands**

This section describes the commands you use to configure IPv6 ACL settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

**ipv6 access-list**

This command creates an IPv6 Access Control List (ACL) identified by `<name>`, consisting of classification fields defined for the IP header of an IPv6 frame. The `<name>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.
If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

**Note:** The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

**Format**

```
ipv6 access-list <name>
```

**Mode**

Global Config

**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

**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

**{deny | permit} (IPv6)**

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list.

**Note:** The `no` form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

**Note:** An implicit 'deny all' IPv6 rule always terminates the access list.
A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the ‘every’ keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword ‘any’ to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <queue-id> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The assign-queue parameter is valid only for a permit rule.

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 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.

Format

{deny | permit} {every | {{icmp | igmp | ipv6 | tcp | udp | <number>}[log] [timerange <time-range-name>] [assign-queue <queue-id>] [{mirror | redirect} <unit/slot/port>]

Mode

IPv6-Access-List Config

ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by <name> to an interface or associates with a VLAN ID in a given direction. The <name> parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified IPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The vlan keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.
Note: You should be aware that the <out> option may or may not be available, depending on the platform.

**no ipv6 traffic-filter**

This command removes an IPv6 ACL identified by <name> from the interface(s) in a given direction.

Format:  
\[ \text{no ipv6 traffic-filter } <\text{name}> [\text{vlan } <\text{vlan-id}>] \in [\text{sequence } <1-4294967295>] \]

Modes:  
- Global Config
- Interface Config

**show ipv6 access-lists**

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the [name] parameter to identify a specific IPv6 ACL to display.

Format:  
\[ \text{show ipv6 access-lists } [\text{name}] \]

Mode:  
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 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 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>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>
</tbody>
</table>
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 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.

\textit{time-range}

Use this command to create a time range identified by \textit{name}, consisting of one absolute time entry and/or one or more periodic time entries. The \textit{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.

\textbf{Note:} When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

\begin{tabular}{|l|l|}
\hline
\textbf{Term} & \textbf{Definition} \\
\hline
IP DSCP & The value specified for IP DSCP. \\
Flow Label & The value specified for IPv6 Flow Label. \\
Log & Displays when you enable logging for the rule. \\
Assign Queue & The queue identifier to which packets matching this rule are assigned. \\
Mirror Interface & The unit/slot/port to which packets matching this rule are copied. \\
Redirect Interface & The unit/slot/port to which packets matching this rule are forwarded. \\
Time Range Name & Displays the name of the time-range if the IPv6 ACL rule has referenced a time range. \\
Rule Status & Status(Active/Inactive) of the IPv6 ACL rule. \\
\hline
\end{tabular}

Format: \texttt{time-range <name>}

Mode: Global Config
no time-range

Use this command to delete a time-range identified by `name`.

**Format**

```
no time-range <name>
```

**Mode**

Global Config

**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

no absolute

Use this command to delete the absolute time entry in the time range.

**Format**

```
no absolute
```

**Mode**

Time-Range Config

**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.

The frequency is how often this periodic entry will become active. If the value is set to 0, timer schedule will be treated as absolute.

**Format**

```
periodic <frequency> {days-of-the-week time} to {days-of-the-week time}
```

**Mode**

Time-Range Config

**no periodic**

Use this command to delete a periodic time entry from a time range.

**Format**

```
no periodic <frequency>{days-of-the-week time} to {days-of-the-week time}
```

**Mode**

Time-Range Config

**periodic {start|end} time**

Use this command to configure the start/end time for the time-range.

**Format**

```
periodic {start|end} time
```

**Mode**

Time-Range Config

**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
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Time Ranges</td>
<td>Number of time ranges configured in the system.</td>
</tr>
<tr>
<td>Time Range Name</td>
<td>Name of the time range.</td>
</tr>
<tr>
<td>Time Range Status</td>
<td>Status of the time range (active/inactive).</td>
</tr>
<tr>
<td>Absolute start</td>
<td>Start time and day for absolute time entry.</td>
</tr>
<tr>
<td>Absolute end</td>
<td>End time and day for absolute time entry.</td>
</tr>
<tr>
<td>Periodic Entries</td>
<td>Number of periodic entries in a time-range.</td>
</tr>
</tbody>
</table>
Auto-VoIP over IP Commands

This section describes the commands you use to configure Auto-VoIP 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.

`auto-voip all`

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

- **Default:** disabled
- **Format:** `auto-voip all`
- **Mode:** Global Config

`no auto-voip all`

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

- **Format:** `no auto-voip all`
- **Mode:** Global Config

`auto-voip`

Use this command to enable VoIP Profile on the interface.

- **Default:** disabled
- **Format:** `auto-voip`
- **Mode:** Interface Config
no auto-voip

Use this command to disable VoIP Profile on the interface.

Format: no auto-voip all

Mode: Interface Config

show auto-voip

Use this command to display the VoIP Profile settings on the interface or interfaces of the switch.

Format: show auto-voip interface {<unit/slot/port>|all}

Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoVoIP Mode</td>
<td>The Auto VoIP mode on the interface.</td>
</tr>
<tr>
<td>Traffic Class</td>
<td>The CoS Queue or Traffic Class to which all VoIP traffic is mapped to. This is not configurable and defaults to the highest CoS queue available in the system for data traffic.</td>
</tr>
</tbody>
</table>
This chapter contains the following sections:

- About PoE
- PoE Commands

**About PoE**

Power over Ethernet describes a technology to pass electrical power safely along with data on existing Ethernet cabling. The PSE or power supply equipment is the device or switch that delivers electrical power, and the PD or powered device is the end device that powers up through the power delivered along the Ethernet cable.

This technology is governed by two standards:

- IEEE 802.3af-2003. This is the original standard, also known as the low power standard, which mandates delivery of up to 15.4 watts by the PSE. Because of power dissipation, only 12.95 watts is assured to be available at the powered device (PD). The PD needs to be designed so that it can accept power over Ethernet cabling. Category 3 cables can be used to deliver power to the PD. However, with the advent of 802.11n, the newer wireless APs required more power. To account for this, a newer standard was developed in 2009, known as 802.3at.

- IEEE 802.3at-2009. This is the newer standard, also known as PoE+. This is also known as the high-power standard, which mandates delivery of up to 34.2 watts by the PSE. Because of power dissipation, PoE+ provides only a maximum of 25.5 watts at the powered device. Some PSEs can provide up to 51 watts. Before this standard became available in 2009, the industry started using different implementations to allow for more power. All these needed to be brought under the purview of the newer 802.3at standard.
PoE Commands

poe

Use this command to enable the Power over Ethernet (PoE) functionality on a global basis or per interface.

Format: poe
Mode: Global Config
        Interface Config
Default: enabled

no poe

Use this command to disable the Power over Ethernet (PoE) functionality on a global basis or per interface.

Format: no poe
Mode: Global Config
        Interface Config

poe detection

Use this command to configure the detection type on a global basis or per interface. It is used to configure which types of PDs will be detected and powered by the switch. There are three options:

- ieee—Detect resistive-type devices (IEEE standard)
- pre-ieee—Legacy capacitive detection only (non-standard)
- auto—Perform resistive detection first (IEEE standard), and then capacitive detection (pre-IEEE standard)

Format: poe detection [ ieee | pre-ieee | auto]
Mode: Global Config
        Interface Config
Default: auto
no poe detection

Use this command to set the detection mode to the default on a global basis or per interface.

Format: no poe detection
Mode: Global Config, Interface Config

poe high-power

Use this command to switch a port from 802.3af mode to high-power mode. This mode is used to power up devices that require more power than the current IEEE 802.3af power (more than 12.95 watts at the PD). There are three options:

- **legacy**—Use this mode if the device can power up (more than 12.95 watts) with higher current and it cannot identify itself as a Class 4 device.
- **Pre-dot3at**—Use this mode if the device cannot identify itself as a Class 4 device and it does not have LLDP support.
- **Dot3at**—Use this mode if the device is a Class 4 device capable of figuring out power requirements through 2-event classification or LLDP.

Format: poe high-power {legacy | pre-dot3at | dot3at}
Mode: Interface Config
Default: dot3at

no poe high-power

Use this command to disable the high-power mode. The port will support only IEEE 902.3af devices.

This command works on a global basis or per interface.

Format: no poe high-power
Mode: Interface Config

poe power limit

Use this command to configure the type of power limit for a port. If the power limit type is “user-defined,” the command also allows you to configure a maximum power limit.

There are three options:

- **class-based**—Allows the port to draw up to the maximum power based on the classification of the device connected.
- **none**—Allows the port to draw up to Class 0 maximum power if it is in low-power mode and up to Class 4 maximum power if it is in high-power mode.
• **user-defined**—Allows you to define the maximum power to the port. This can be a value between 3 and 32 watts.

**Format**
```
poe power limit { class-based | none | user-defined [<3000 - 32000>]} 
```

**Mode**
- Global Config
- Interface Config

**Default**
User-defined, with a maximum of 30 watts

**no poe power limit**

Use this command to set the power limit type to the default. It also sets the maximum power limit to the default if the power limit type is user-defined.

**Format**
```
no poe power limit [user-defined] 
```

**Mode**
- Global Config
- Interface Config

**poe power management**

Use this command to configure the power management mode based on each individual PoE unit or on all PoE units.

Both the power management modes mentioned here will power up a device based on first come, first served. When the available power is less than the power limit defined on a port, no more power will be delivered.

Static and dynamic modes differ in how the available power is calculated, as follows:

**Static Power Management**

Available power = power limit of the source - total allocated power

Where total allocated power is calculated as the power limit configured on the port.

**Dynamic Power Management**

Available power = power limit of the source - total allocated power

Where total allocated power is calculated as the amount of power consumed by the port.

For example:

Assume that the power limit of the source is 300 watts. One port is powered up and is drawing 3 watts of power. The power limit defined on the port is user-defined as 15 watts. In this case, the available power for static and dynamic would be as follows:

**Static Power Management**

Available power = 300 watts - 15 watts = 285 watts
Dynamic Power Management

Available power = 300 watts - 3 watts = 297 watts

**Format**
poe power management {<unit>|all} {dynamic | static}

**Mode**
Global Config

**Default**
dynamic

**no poe power management**

Use this command to set the power management mode to the default.

**Format**
no poe power management {<unit>|all}

**Mode**
Global Config

**poe priority**

Use this command to configure the priority on a specific port. This is used for power management purposes. The switch might 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 will have higher priority. There are three options:

- **Crit**—Critical priority
- **High**—High priority
- **Low**—Low priority

**Format**
poe priority { Crit | High | Low }

**Mode**
Global Config
Interface Config

**Default**
low

**no poe priority**

Use this command to set the priority to the default.

**Format**
no poe priority

**Mode**
Global Config
Interface Config

**poe reset**

Use this command to reset the PoE state of every port (in global mode) or a specific port (in interface mode). When the PoE port status is shown to be in an error state, this command can be
used to reset the PoE port. The command can also reset the power-delivering ports. Note that this command takes effect only once after it is executed and cannot be saved across power cycles.

```
Format  poe reset
Mode    Global Config
        Interface Config
```

**poe reset auto**

Use this command to set the auto-reset mode. When auto-reset mode is enabled, the PoE port will be automatically reset if an error, such as overload, is detected on the port. By default the auto reset mode is enabled. This command allows you to set the mode based on each individual PoE unit or all PoE units.

```
Format  poe reset auto {<unit>|all}
Mode    Global Config
Default Enable
```

**no poe reset auto**

Use this command to clear autoreset mode.

```
Format  no poe reset auto {<unit>|all}
Mode    Global Config
```

**poe timer schedule name**

Use this command to allow you to attach a timer schedule to a PoE port.

You can define a time schedule using the existing time range commands. This schedule has start and stop times. When this timer schedule is applied to a PoE-enabled port, the capability of the port to deliver power is affected. At the scheduled start time, the PoE port is disabled such that it cannot deliver any power. At the scheduled stop time, the PoE port is reenabled so that it can deliver power.

---

**Note:** For information about creating a timer schedule, see *Time Range Commands for Time-Based ACLs* on page 485.

```
Format  poe timer schedule <name>
Mode    Interface Config
```

---
**no poe timer schedule name**

Use this command to detach the schedule from the port.

**Format**

```
no poe timer schedule
```

**Mode**

Interface Config

**poe usagethreshold**

Use this command to set a threshold (as a percentage) for the total amount of power that can be delivered by the switch. For example, if the switch can deliver up to a maximum of 300 watts, a usage threshold of 90% ensures that only 270 watts are used for delivering power to devices. This ensures that more power is not drawn than the switch can provide.

When the usage threshold is set, all the PDs are brought down and then brought back up. If the consumed power is less than the threshold power (in the preceding case, 270 watts), then the devices continue to power up. If the consumed power is 269 watts or less, the next device is powered up. The moment consumed power exceeds the threshold power (270 watts), no other devices can power up.

This command allows you to set the usage threshold based on each individual PoE unit or all PoE units.

**Format**

```
poe usagethreshold {<unit>|all} <1-99>
```

**Mode**

Global Config

**Default**

90

**no poe usagethreshold**

Use this command to set the usage threshold to a default value.

**Format**

```
no poe usagethreshold {<unit>|all}
```

**Mode**

Global Config

**poe traps**

Use this command to enable logging of specific PoE-related events, such as a PoE port powering a device, the threshold being exceeded, and so on.

**Format**

```
poe traps
```

**Mode**

Global Config

**Default**

Enable
**no poe traps**

Use this command to disable logging the PoE traps.

**Format**

```
no poe traps
```

**Mode**

- Global Config

**show poe**

Use this command to get global information regarding the PoE status.

**Format**

```
show poe
```

**Mode**

- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firmware Version</strong></td>
<td>This is the firmware version of the PoE controller on the switch.</td>
</tr>
</tbody>
</table>
| **PSE Main Operational Status** | This indicates the status of the PoE controller:  
  - ON—Indicates that the PoE controller is actively delivering power.  
  - OFF—Indicates that the PoE controller is not delivering power.  
  - FAULTY—Indicates that the PoE controller is not functioning. |
| **Total Power (Main AC)** | This indicates the maximum amount of power that can be delivered by this PoE unit when on system power. |
| **Total Power (RPS)**    | This indicates the maximum amount of power that can be delivered by this PoE unit when on RPS. |
| **Total Power (PD)**     | This indicates the maximum amount of power that can be delivered by this PoE unit when on the PD source. This field is applicable only for the GSM5212P. |
| **Power Source**         | This indicates the power source being used: main AC, RPS, or PD. If PD is used as a source, then “PD <portNo>” is displayed. |
| **Threshold Power**      | System can power up one port, if consumed power is less than this power. That is, the consumed power can be between the total power and threshold power values. The threshold power value is effected by changing the system usage threshold. |
| **Total Power Consumed** | This indicates the total amount of power being delivered to all the devices plugged into the switch. |
| **Usage Threshold**      | This indicates the usage threshold level.                                  |
| **Power Management Mode** | This indicates the management mode used by the PoE controller.              |
| **Auto Reset Mode**      | This indicates whether the PoE ports will be automatically reset in case of an error on a port. |
| **Traps**                | This configures the traps.                                                 |
Example:

(switch) #show poe

Firmware Version............................... 1.0.0.2
PSE Main Operational Status.................... ON
Total Power (Main AC).......................... 380
Total Power (RPS).............................. 300
Total Power (PD) .............................. 25
Power Source................................... Main AC
Threshold Power................................ 342
Total Power Consumed........................... 7
Usage Threshold................................. 90
Power Management Mode......................... Dynamic
Configure port Auto Reset Mode................. Disable
Traps.......................................... Enable

**show poe port configuration**

Use this command to see how the PoE ports are configured. You can display information based on each individual port or all the ports collectively.

**Format**

show poe port configuration [<port> |All]

**Mode**

Privileged EXEC
User EXEC

(Switch) #show poe port configuration all

<table>
<thead>
<tr>
<th>Intf</th>
<th>Admin</th>
<th>Mode</th>
<th>Priority</th>
<th>Power Limit</th>
<th>High Power</th>
<th>Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>(W)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/0/1</td>
<td>Enable</td>
<td>Low</td>
<td>15.400</td>
<td>User Defined</td>
<td>Disable</td>
<td>Auto</td>
</tr>
<tr>
<td>1/0/2</td>
<td>Enable</td>
<td>Low</td>
<td>15.400</td>
<td>User Defined</td>
<td>Disable</td>
<td>Auto</td>
</tr>
</tbody>
</table>

(Switch) #show poe port configuration 1/0/2

<table>
<thead>
<tr>
<th>Intf</th>
<th>Admin</th>
<th>Mode</th>
<th>Priority</th>
<th>Power Limit</th>
<th>High Power</th>
<th>Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>(W)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/0/2</td>
<td>Enable</td>
<td>Low</td>
<td>15.400</td>
<td>User Defined</td>
<td>Disable</td>
<td>Auto</td>
</tr>
</tbody>
</table>
**show poe port info**

Use this command to get information about the status of the PoE ports. You can display information based on each individual port or all the ports collectively. The command displays only PSE-capable ports.

**Format**

```
show poe port info [<port> | all]
```

**Mode**

Privileged EXEC

User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf</td>
<td>Interface on which PoE is configured.</td>
</tr>
<tr>
<td>Class</td>
<td>Class of the powered device according to the IEEE802.3af and IEEE802.3at definition.</td>
</tr>
<tr>
<td></td>
<td>Class Usage Max Power (watts)</td>
</tr>
<tr>
<td></td>
<td>Default 0.44-12.95</td>
</tr>
<tr>
<td></td>
<td>Optional 0.44-3.84</td>
</tr>
<tr>
<td></td>
<td>Optional 3.84-6.49</td>
</tr>
<tr>
<td></td>
<td>Optional 6.49-12.95</td>
</tr>
<tr>
<td></td>
<td>Optional 12.95-25.5</td>
</tr>
<tr>
<td>Power</td>
<td>The power supplied to the powered device (in watts).</td>
</tr>
<tr>
<td>Output Current (mA)</td>
<td>The current supplied to the powered device (in mA).</td>
</tr>
<tr>
<td>Output Voltage (volts)</td>
<td>The voltage supplied to the powered device (in volts).</td>
</tr>
<tr>
<td>Status</td>
<td>The Status field reports the state of power supplied to the port. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>- Disabled—The PoE function is disabled on this port.</td>
</tr>
<tr>
<td></td>
<td>- Searching—The port is detecting the PoE device.</td>
</tr>
<tr>
<td></td>
<td>- Delivering Power—The port is providing power to the PoE device.</td>
</tr>
<tr>
<td></td>
<td>- Fault—The POE device is not IEEE compliant; no power is provided.</td>
</tr>
<tr>
<td></td>
<td>- Test—The port is in testing state.</td>
</tr>
<tr>
<td></td>
<td>- Other Fault—The port has experienced problems other than compliance issues.</td>
</tr>
</tbody>
</table>

Example:

```
(switch) #show poe port info all

High       Max                    Output    Output
Intf   Power     Power   Class   Power    Current   Voltage      Status            Fault
------ -------  -----  -------  ------  -------    -------   ------------------ ---------------
1/0/1    Yes     32.0   Unknown   00.000   0         00.00      Searching          No Error

(Switch) #show poe port info 1/0/33

High    Max       Output    Output
------  -------  -------  -------
Yes     32.0    00.000    00.00
```
show poe pd

Use this command to get information about the PD ports. You can display information based on each individual port or all the PD ports collectively.

**Note:** Only the GSM5212P supports this command.

| Format | show poe pd [<port> | all] |
|--------|-------------------|
| Mode   | Privileged EXEC   |
|        | User EXEC         |

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf</td>
<td>Show the PD device interface number, only 0/1 or 0/2 on the GSM5212P. In other devices, the table is empty. If &lt;port-id&gt; is not specified, all PD ports are displayed.</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the port POE role and is always PD.</td>
</tr>
<tr>
<td>Class</td>
<td>Displays the POE class.</td>
</tr>
<tr>
<td>Detection Mode</td>
<td>PD detection mode when getting power from the PSE:</td>
</tr>
<tr>
<td></td>
<td>1-event—PSE detects the PD in 1-event mode (802.1f)</td>
</tr>
<tr>
<td></td>
<td>2-event—PSE detects the PD in 2-event mode (802.1at)</td>
</tr>
<tr>
<td></td>
<td>LLDP—PSE detects the PD in LLDP mode (802.1at)</td>
</tr>
<tr>
<td>Status</td>
<td>Shows whether the port 0/1 or 0/2 is providing power:</td>
</tr>
<tr>
<td></td>
<td>Powered—Receiving power from PSE</td>
</tr>
<tr>
<td></td>
<td>Off—No power from the PSE (when main AC is in used)</td>
</tr>
</tbody>
</table>

Example:

```
(switch) #show poe pd all
```

<table>
<thead>
<tr>
<th>Intf</th>
<th>Mode</th>
<th>Class</th>
<th>Detection Mode</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
<td>PD</td>
<td>class 4</td>
<td>2-event</td>
<td>powered</td>
</tr>
<tr>
<td>0/2</td>
<td>PD</td>
<td>class 4</td>
<td>LLDP</td>
<td>powered</td>
</tr>
</tbody>
</table>
This chapter describes the utility commands available in the CLI.

This chapter contains the following sections:

- Auto Install Commands
- Dual Image Commands
- System Information and Statistics Commands
- Logging Commands
- Email Alerting and Mail Server Commands
- System Utility and Clear Commands
- Simple Network Time Protocol (SNTP) Commands
- DHCP Server Commands
- DNS Client Commands
- Packet Capture Commands
- Serviceability Packet Tracing Commands
- Cable Test Command
- sFlow Commands
- Software License Commands
- IP Address Conflict Commands
- Link Local Protocol Filtering Commands

The commands in this chapter are in 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.
Auto Install Commands

This section describes the Auto Install Commands. Auto Install is a software feature which provides for the configuration of a switch automatically when the device is initialized and no configuration file is found on the switch. The Auto Install process requires DHCP to be enabled by default in order for it to be completed. The downloaded config file is not automatically saved to startup-config. An administrator must explicitly issue a save request in order to save the configuration. The Auto Install process depends upon the configuration of other devices in the network, including a DHCP or BOOTP server, a TFTP server and, if necessary, a DNS server.

There are three steps to Auto Install:

1. Configuration or assignment of an IP address for the device.
2. Assignment of a TFTP server.
3. Obtain a configuration file for the device from the TFTP server.

show autoinstall

This command displays the current status of the Auto Config process.

<table>
<thead>
<tr>
<th>Format</th>
<th>show autoinstall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoInstall Mode</td>
<td>The administrator mode is enabled or disabled.</td>
</tr>
<tr>
<td>AutoSave Mode</td>
<td>If this option is enabled, the downloaded config file will be saved. Otherwise, administrator must explicitly issue a &quot;copy running-config startup-config&quot; command in order to save the configuration.</td>
</tr>
<tr>
<td>AutoInstall Retry Count</td>
<td>the number of attempts to download a configuration.</td>
</tr>
<tr>
<td>AutoInstall State</td>
<td>The status of the AutoInstall.</td>
</tr>
</tbody>
</table>

Example

(switch) #show autoinstall
AutoInstall Mode......................... Stopped
AutoSave Mode............................ Disabled
AutoInstall Persistent Mode............. Enabled
AutoInstall Retry Count............... 3
AutoInstall State....................... Waiting for boot options
**boot host auto-save**

This command is used to enable automatically saving the downloaded configuration on the switch.

**Default**  
Disabled

**Format**  
boot host auto-save

**Mode**  
Privileged EXEC

**no boot host auto-save**

This command is used to disable automatically saving the downloaded configuration on the switch.

**Format**  
no boot host auto-save

**Mode**  
Privileged EXEC

**boot autoinstall start**

The command is used to start Auto Install on the switch. Auto Install tries to download a config file from a TFTP server.

**Format**  
boot autoinstall start

**Mode**  
Privileged EXEC

**boot autoinstall stop**

The command is used to A user may terminate the Auto Install process at any time prior to the downloading of the config file. This is most optimally done when the switch is disconnected from the network, or if the requisite configuration files have not been configured on TFTP servers. Termination of the Auto Install process ends further periodic requests for a host-specific file.

**Format**  
boot autoinstall stop

**Mode**  
Privileged EXEC

**boot host retry-count**

This command is used to set the number of attempts to download a configuration. The valid range is from 1 to 6.

**Default**  
3

**Format**  
boot host retry-count <count>

**Mode**  
Privileged EXEC
**no boot host retry-count**

This command is used to reset the number to the default. The default number is 3.

**Format**
```
no boot host retry-count
```

**Mode**
Privileged EXEC

**boot host dhcp**

This command is used 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

**no boot host dhcp**

This command is used to disable 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.

**Format**
```
no boot host dhcp
```

**Mode**
Privileged EXEC

---

**Dual Image Commands**

The 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.

**delete**

This command deletes the supplied image file from the permanent storage. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, an error message displays. The optional `<unit>` parameter is valid only on Stacks. Error will be returned, if this parameter is provided, on Standalone systems. In a stack, the `<unit>` parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

**Format**
```
delete [<unit>] {image1 | image2}
```

**Mode**
Privileged EXEC
**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. The optional `<unit>` parameter is valid only in Stacking, where the `unit` parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

**Format**

```
boot system [<unit>] <image-file-name>
```

**Mode**

Privileged EXEC

**show bootvar**

This command displays the version information and the activation status for the current active and backup images on the supplied unit (node) of the Stack. If you do not specify a unit number, the command displays image details for all nodes on the Stack. The command also displays any text description associated with an image. This command, when used on a Standalone system, displays the switch activation status. For a standalone system, the unit parameter is not valid.

**Format**

```
show bootvar [<unit>]
```

**Mode**

Privileged EXEC

**filedescr**

This command associates a given text description with an image. Any existing description will be replaced. For stacking, the `[<unit>]` parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

**Format**

```
filedescr [<unit>] {image1 | image2} <text-description>
```

**Mode**

Privileged EXEC

**update bootcode**

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots. The optional `<unit>` parameter is valid only on Stacks. Error will be returned, if this parameter is provided, on Standalone systems. For Stacking, the `<unit>` parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

**Format**

```
update bootcode [<unit>]
```

**Mode**

Privileged EXEC
System Information and Statistics Commands

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

**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.

<table>
<thead>
<tr>
<th>Format</th>
<th>show arp switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<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 <em>Management</em>. For a network port, the output is the unit/slot/port of the physical interface.</td>
</tr>
</tbody>
</table>

**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. The `<unit>` is the switch identifier.

<table>
<thead>
<tr>
<th>Format</th>
<th>show eventlog <code>&lt;unit&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>The file in which the event originated.</td>
</tr>
<tr>
<td>Line</td>
<td>The line number of the event.</td>
</tr>
<tr>
<td>Task Id</td>
<td>The task ID of the event.</td>
</tr>
<tr>
<td>Code</td>
<td>The event code.</td>
</tr>
<tr>
<td>Time</td>
<td>The time this event occurred.</td>
</tr>
<tr>
<td>Unit</td>
<td>The unit for the event.</td>
</tr>
</tbody>
</table>

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

This command displays inventory information for the switch.

**Note:** The show version command and the show hardware command display the same information. In future releases of the software, the show hardware command will not be available. For a description of the command output, see the command show version on page 507.

**Format**  
show hardware

**Mode**  
Privileged EXEC

show version

This command displays inventory information for the switch.

**Note:** The show version command will replace the show hardware command in future releases of the software.

**Format**  
show version

**Mode**  
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Description</td>
<td>Text used to identify the product name of this switch.</td>
</tr>
<tr>
<td>Machine Type</td>
<td>The machine model as defined by the Vital Product Data.</td>
</tr>
<tr>
<td>Machine Model</td>
<td>The machine model as defined by the Vital Product Data.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The unique box serial number for this switch.</td>
</tr>
<tr>
<td>FRU Number</td>
<td>The field replaceable unit number.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Manufacturer descriptor field.</td>
</tr>
<tr>
<td>Burned in MAC Address</td>
<td>Universally assigned network address.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The release.version.revision number of the code currently running on the switch.</td>
</tr>
<tr>
<td>Additional Packages</td>
<td>The additional packages incorporated into this system.</td>
</tr>
</tbody>
</table>
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 {<unit/slot/port> | switchport}
Mode    Privileged EXEC

The display parameters, when the argument is <unit/slot/port>, are as follows:

<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>Packets Transmitted Without Error</td>
<td>The total number of packets transmitted out of the interface.</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>
</tbody>
</table>
**show interface ethernet**

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

**Format**

```
show interface ethernet [<unit/slot/port> | switchport]
```

**Mode**

Privileged EXEC

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Packets Received (Octets)</td>
<td>The total number of octets of data received by the processor (excluding framing bits but including FCS octets).</td>
</tr>
<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>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 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 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. A possible reason for discarding a packet could be to free up buffer space.</td>
</tr>
<tr>
<td>Octets Transmitted</td>
<td>The total number of octets transmitted out of the interface, including framing characters.</td>
</tr>
<tr>
<td>Packets Transmitted without Errors</td>
<td>The total number of packets transmitted out of the interface.</td>
</tr>
<tr>
<td>Unicast Packets Transmitted</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 <unit/slot/port> parameter to view MAC addresses on a specific interface. Use the vlan <vlan_id> parameter to display information about MAC addresses on a specified VLAN.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.</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 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>Most Address Entries Ever Used</td>
<td>The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.</td>
</tr>
<tr>
<td>Address Entries Currently in Use</td>
<td>The number of Learned and static entries in the Forwarding Database Address Table for this switch.</td>
</tr>
<tr>
<td>Maximum VLAN Entries</td>
<td>The maximum number of Virtual LANs (VLANs) allowed on this switch.</td>
</tr>
<tr>
<td>Most VLAN Entries Ever Used</td>
<td>The largest number of VLANs that have been active on this switch since the last reboot.</td>
</tr>
<tr>
<td>Static VLAN Entries</td>
<td>The number of presently active VLAN entries on this switch that have been created statically.</td>
</tr>
<tr>
<td>Dynamic VLAN Entries</td>
<td>The number of presently active VLAN entries on this switch that have been created by GVRP registration.</td>
</tr>
<tr>
<td>VLAN Deletes</td>
<td>The number of VLANs on this switch that have been created and then deleted since the last reboot.</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>

Format: show mac-addr-table [{<macaddr> <vlan_id> | all | count | interface <unit/slot/port> | vlan <vlan_id>}]
The following information displays if you do not enter a parameter, the keyword all, or the MAC address and VLAN ID. If you enter `vlan <vlan_id>`, only the Mac Address, Interface, and Status fields appear.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Address</td>
<td>A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.</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 the `interface <unit/slot/port>` parameter, in addition to the MAC Address and Status fields, the following field appears:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN on which the MAC address was learned.</td>
</tr>
</tbody>
</table>

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>
**show process cpu**

This command provides the percentage utilization of the CPU by different tasks.

**Note:** It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

**Format**  
`show process cpu`

**Mode**  
Privileged EXEC

The following shows example CLI display output.

(Switch) #show process cpu

Memory Utilization Report
status bytes
------  ---------
free  192980480
alloc 53409968

Task Utilization Report
Task Utilization
-----------------------  -----------
bcmL2X.0                      0.75%
bcmCNTR.0                     0.20%
bcmLINK.0                     0.35%
DHCP snoop                    0.10%
Dynamic ARP Inspection        0.10%
dotls_timer_task              0.10%
dhcpsPingTask                 0.20%

**show mbuf total**

This command shows the total system buffer pools status.

**Format**  
`show mbuf total`

**Mode**  
Privileged EXEC

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

(switch) #show mbuf total

mbufSize 9284 (0x2444)
Current Time 0x1897fa
MbufsFree 150
MbufsRxUsed 0
Total Rx Norm Alloc Attempts 26212
Total Rx Mid2 Alloc Attempts 4087
Total Rx Mid1 Alloc Attempts 188943
show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the `[all]` option.

**Note:** Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional `<scriptname>` is provided with a file name extension of “.scr”, the output is redirected to a script file.

**Note:** If you issue the show running-config command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

**Note:** If you use a text-based configuration file, the `show running-config` command will only display configured physical interfaces, i.e. if any interface only contains the default configuration, that interface will be skipped from the `show running-config` command output. This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its ‘exit’ command, are both omitted from the `show running-config` command output (and hence from the startup-config file when the system configuration is saved.)

If option `<changed>` is used, this command displays/capture commands with settings/configurations that differ from the default value.
• 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> | changed]`

**Mode**
Privileged EXEC

### show running-config interface

This command shows the current configuration on a particular interface. The interface could be a physical port or a virtual port—like a LAG or VLAN. The output captures how the configuration differs from the factory default value.

**Format**
`show running-config interface {<unit/slot/port> | VLAN <id> | LAG <id>}`

**Mode**
Interface Config

### 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 <code>snmp-server</code> on page 628.</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 <code>snmp-server</code> on page 628.</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 <code>snmp-server</code> on page 628.</td>
</tr>
<tr>
<td>System Object ID</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>MIbs Supported</td>
<td>A list of MIbs supported by this agent.</td>
</tr>
</tbody>
</table>

### show tech-support

Use the `show tech-support` command to display system and configuration information when you contact technical support. The output of the `show tech-support` command combines the output of the following commands:
• show version
• show sysinfo
• show port all
• show isdp neighbors
• show logging
• show event log
• show logging buffered
• show trap log

Format: show tech-support
Mode: Privileged EXEC

terminal length

Use this command to set the number of lines of output to be displayed on the screen, i.e. pagination, for the show running-config and show running-config all commands. The terminal length size is either zero or a number in the range of 5 to 48. After the user-configured number of lines is displayed in one page, the system prompts the user “--More-- or (q)uit.” Press q or Q to quit, or press any key to display the next set of <5-48> lines. The command terminal length 0 disables pagination and, as a result, the output of the show running-config command is displayed immediately.

Default: 24 lines per page
Format: terminal length <0|5-48>
Mode: Privileged EXEC

no terminal length

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

Format: no terminal length
Mode: Privileged EXEC

show terminal length

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

Format: show terminal length
Mode: Privileged EXEC
Logging Commands

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

**logging buffered**

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

Default: disabled; critical when enabled

Format: `logging buffered`

Mode: Global Config

**no logging buffered**

This command disables logging to in-memory log.

Format: `no logging buffered`

Mode: Global Config

**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

**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

**logging cli-command**

This command enables the CLI command logging feature, which enables the 7000 series software to log all CLI commands issued on the system.

Default: enabled
**Utility Commands**

**Format**

- `logging cli-command`

**Mode**

- Global Config

---

**no logging cli-command**

This command disables the CLI command Logging feature.

**Format**

- `no logging cli-command`

**Mode**

- Global Config

---

**logging console**

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

**Default**

- disabled; critical when enabled

**Format**

- `logging console [severitylevel]`

**Mode**

- Global Config

---

**no logging console**

This command disables logging to the console.

**Format**

- `no logging console`

**Mode**

- Global Config

---

**logging host**

This command enables logging to a host. You can configure up to eight hosts. The `<ipaddr|hostname>` is the IP address of the logging host. The `<addressstype>` indicates the type of address ipv4 or ipv6 or dns being passed. The `<port>` value is a port number from 1 to 65535. You can specify the `<severitylevel>` value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

**Default**

- port—514
- level—critical (2)

**Format**

- `logging host <ipaddr|hostname> <addressstype> <port> [severitylevel]`

**Mode**

- Global Config
logging host remove

This command disables logging to host. See show logging hosts on page 519 for a list of host indexes.

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

logging syslog

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

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

no logging syslog

This command disables syslog logging.

Format:  no logging syslog
Mode:    Global Config

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>CLI Command Logging</td>
<td>Shows whether CLI Command logging is enabled.</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>
<tr>
<td>Buffered Logging</td>
<td>Shows whether buffered logging is enabled.</td>
</tr>
<tr>
<td>Syslog Logging</td>
<td>Shows whether syslog logging is enabled.</td>
</tr>
</tbody>
</table>
show logging buffered

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

Format: `show logging buffered`
Mode: Privileged EXEC

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

show logging hosts

This command displays all configured logging hosts. The `<unit>` is the switch identifier and has a range of 1-8.

Format: `show logging hosts <unit>`
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>Host Status</td>
<td>The state of logging to configured syslog hosts. If the status is disable, no logging occurs.</td>
</tr>
</tbody>
</table>
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>

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

no logging persistent

Use this command to disable the persistent logging in the switch.

Format  no logging persistent
Mode  Global Config

Email Alerting and Mail Server Commands

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 will be emailed.
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 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; when enabled, log messages at or above severity Warning (4) are emailed
Format | logging email [<severitylevel>]
Mode | Global Config

**no logging email**

This command disables email alerting.

Format | no logging email
Mode | Global Config

**logging email urgent**

This command sets the lowest severity level at which log messages are emailed immediately in a single email message. 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). 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

**no logging email urgent**

This command resets the urgent severity level to the default value.

Format | no logging email urgent
Mode | Global Config

**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
**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

---

**logging email from-addr**

This command configures the email address of the sender (the switch).

**Default**

switch@netgear.com

**Format**

```
logging email from-addr <from-email-addr>
```

**Mode**

Global Config

---

**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

---

**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

---

**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
**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

**no logging email logtime**

This command resets the non-urgent log time to the default value.

Format: `no logging email logtime`

Mode: Global Config

**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

**no logging traps**

This command resets the SNMP trap logging severity level to the default value.

Format: `no logging traps`

Mode: Global Config

**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
**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</td>
</tr>
<tr>
<td></td>
<td>are sent immediately.</td>
</tr>
<tr>
<td>Email Alert Non Urgent Severity</td>
<td>The lowest severity level that is considered non-urgent. Messages of this</td>
</tr>
<tr>
<td>Level</td>
<td>type, up to the urgent level, are collected and sent in a batch email.</td>
</tr>
<tr>
<td></td>
<td>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)</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>The configured email subject for sending non-urgent messages.</td>
</tr>
</tbody>
</table>

**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</td>
</tr>
<tr>
<td></td>
<td>unsuccessful.</td>
</tr>
</tbody>
</table>
clear logging email statistics

This command resets the email alerting statistics.

**Format**
clear logging email statistics

**Mode**
Privileged EXEC

mail-server

Use this command to configure the SMTP server to which the switch sends email alert messages and change 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

no mail-server

Use this command to remove the specified SMTP server from the configuration.

**Format**
no mail-server {ip-address | ipv6-address | hostname}

**Mode**
Global Config

Security

Use this command to set 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 sever does not support TLS mode, no email is sent to the SMTP server.

**Default**
none

**Format**
security {tlsv1 | none}

**Mode**
Mail Server Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of Email Sent</td>
<td>The number of email messages that were sent from the switch since the</td>
</tr>
<tr>
<td></td>
<td>counter was cleared.</td>
</tr>
<tr>
<td>Time Since Last Email</td>
<td>The amount of time that has passed since the last email was sent from the</td>
</tr>
<tr>
<td>Sent</td>
<td>switch.</td>
</tr>
</tbody>
</table>
Port

Use this command to configure 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.

Default: 25
Format: `port {465 | 25 | 1-65535}`
Mode: Mail Server Config

Username

Use this command to configure the login ID that the switch uses to authenticate with the SMTP server.

Default: admin
Format: `username name`
Mode: Mail Server Config

Password

Use this command to configure the password that the switch uses to authenticate with the SMTP server.

Format: `password password`
Mode: Mail Server Config

show mail-server config

Use this command to display 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>
</tbody>
</table>
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.

**traceroute**

Use the `traceroute` command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

**Default**

- count: 3 probes
- interval: 3 seconds
- size: 0 bytes
- port: 33434
- maxTtl: 30 hops
- maxFail: 5 probes
- initTtl: 1 hop

**Format**

```
traceroute <ipaddr|hostname> [initTtl <initTtl>] [maxTtl <maxTtl>]
[maxFail <maxFail>] [interval <interval>] [count <count>]
[port <port>] [size <size>]
```

**Mode**

Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>hostname</td>
</tr>
<tr>
<td>initTtl</td>
<td>Use <code>initTtl</code> to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.</td>
</tr>
<tr>
<td>maxTtl</td>
<td>Use <code>maxTtl</code> to specify the maximum TTL. Range is 1 to 255.</td>
</tr>
<tr>
<td>maxFail</td>
<td>Use <code>maxFail</code> to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.</td>
</tr>
<tr>
<td>interval</td>
<td>Use <code>interval</code> to specify the time between probes, in seconds. Range is 1 to 60 seconds.</td>
</tr>
</tbody>
</table>
Utility Commands

ProSafe Managed Switch

Example: The following are examples of the CLI command.

**traceroute Success:**

(Switch) # 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

**traceroute Failure:**

(Switch) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3 port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *

Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18

**traceroute ipv6**

Use the `traceroute` command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The `<ipv6-address|hostname>` parameter must be a valid IPv6 address or hostname. The optional `<port>` parameter is the UDP port used as the destination of packets sent as part of the `traceroute`. This port should be an unused port on the destination system. The range for `<port>` is zero (0) to 65535. The default value is 33434.

**Default**

port: 33434

**Format**

`traceroute ipv6 <ipv6-address|hostname> [port <port>]`

**Mode**

Privileged EXEC
**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

**clear mac-addr-table**

This command clears the dynamically learned MAC addresses of the switch.

**Format**
```
clear mac-addr-table
```

**Mode**
Privileged EXEC

**clear logging buffered**

This command clears the messages maintained in the system log.

**Format**
```
clear logging buffered
```

**Mode**
Privileged EXEC

**clear counters**

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

**Format**
```
clear counters {<unit/slot/port> | all}
```

**Mode**
Privileged EXEC

**clear igmpsnsnooping**

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

**Format**
```
clear igmpsnsnooping
```

**Mode**
Privileged EXEC
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

clear port-channel

This command clears all port-channels (LAGs).

Format  clear port-channel
Mode     Privileged EXEC

clear traplog

This command clears the trap log.

Format  clear traplog
Mode     Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format  clear vlan
Mode     Privileged EXEC

enable password

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case sensitive. The option [encrypted] allows the administrator to transfer the enable password between devices without having to know the password. In this case, the <password> parameter must be exactly 128 hexadecimal characters.

Format  enable password <password> [encrypted]
Mode     Privileged EXEC

logout

This command closes the current telnet connection or resets the current serial connection.
Note: Save configuration changes before logging out.

Format: logout

Modes: Privileged EXEC, User EXEC

**ping**

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces.

Default:
- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format:
```
ping <ipaddress|hostname> [count <count>] [interval <interval>] [size <size>]
```

Modes: Privileged EXEC, User EXEC

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Use the <code>count</code> parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the <code>&lt;ip-address&gt;</code> field. The range for <code>&lt;count&gt;</code> is 1 to 15 requests.</td>
</tr>
<tr>
<td>interval</td>
<td>Use the <code>interval</code> 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 <code>size</code> parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.</td>
</tr>
</tbody>
</table>

The following are examples of the CLI command.

ping success:

```
(Switch) #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
```
ping failure:

In Case of Unreachable Destination:

(Switch) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response: Unreachable Destination
Received Response: Unreachable Destination
----192.168.254.222 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0

In Case Of Request TimedOut:

(Switch) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted, 0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0

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 \textit{ipv6-address|hostname} parameter to ping an interface by using the global IPv6 address of the interface. Use the optional \textit{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 \textit{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 \textit{serviceport} or \textit{network} parameter.

Defaults

- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format

\texttt{ping ipv6 \{<ipv6-global-address|hostname>\} [size <datagram-size>]} 

Modes

- Privileged EXEC
- User EXEC
**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. Use the `interface` keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. You can use a loopback, network port, or physical interface as the source. Use the optional `size` keyword to specify the size of the ping packet. The `ipv6-address` is the link local IPv6 address of the device you want to query.

**Format**

```
ping ipv6 interface {<unit/slot/port> | loopback <loopback-id> | network} <link-local-address> [size <datagram-size>]
```

**Modes**
- Privileged EXEC
- User EXEC

**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

**reload**

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

**Format**

```
reload
```

**Mode**
- Privileged EXEC

**save**

This command makes the current configuration changes permanent by writing the configuration changes to system NVRAM.

**Format**

```
save
```

**Mode**
- Privileged EXEC
**copy**

The **copy** command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (*image1* and *image2*) on the file system. Upload and download files from a server by using TFTP or Xmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management.

**Format**  
```
copy <source> <destination>
```

**Mode**  
Privileged EXEC

Replace the `<source>` and `<destination>` parameters with the options in table below. For the `<url>` source or destination, use one of the following values:

{xmodem | tftp://<ipaddr|hostname>|<ip6address|hostname>/<filepath>/<filename> [noval]  
| sftp|scp://<username>@<ipaddr>|<ipv6address>|<filepath>|<filename>}

For TFTP, SFTP and SCP, the `<ipaddr|hostname>` parameter is the IP address or host name of the server, `<filepath>` is the path to the file, and `<filename>` is the name of the file you want to upload or download. For SFTP and SCP, the `<username>` parameter is the username for logging into the remote server via SSH.

**Note:** `<ip6address>` is also a valid parameter for routing packages that support IPv6.

For switches that support a USB device, the copy command can be used to transfer files from and to the USB device. The syntax for the USB file is: `usb://<filename>`. The USB device can be either a source or destination in the `copy` command. It cannot be used as both source and destination in a given `copy` command.

**Note:** Remember to upload the existing Switch CLI.cfg file off the switch prior to loading a new release image in order to make a backup.

Parameters for the `copy` command are listed in the following table:

<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><code>&lt;url&gt;</code></td>
<td>Copies the CLI banner to a server.</td>
</tr>
<tr>
<td>nvram:errorlog</td>
<td><code>&lt;url&gt;</code></td>
<td>Copies the error log file to a server.</td>
</tr>
<tr>
<td>nvram:Switch CLI.cfg</td>
<td><code>&lt;url&gt;</code></td>
<td>Uploads the binary config file to a server.</td>
</tr>
</tbody>
</table>
### Utility Commands

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nvram:log</td>
<td>&lt;url&gt;</td>
<td>Copies the log file to a server.</td>
</tr>
<tr>
<td>nvram:script &lt;scriptname&gt;</td>
<td>&lt;url&gt;</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>&lt;url&gt;</td>
<td>Copies the startup configuration to a server.</td>
</tr>
<tr>
<td>nvram:traplog</td>
<td>&lt;url&gt;</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>&lt;url&gt;</td>
<td>nvram:clibanner</td>
<td>Downloads the CLI banner to the system.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:Switch CLI.cfg</td>
<td>Downloads the binary config file to the system.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:script &lt;destfilename&gt;</td>
<td>Downloads a configuration script file to the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>During the download of a configuration script, the copy command validates the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>script. In case of any error, the command lists all the lines at the end of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the validation process and prompts you to confirm before copying the script</td>
</tr>
<tr>
<td></td>
<td></td>
<td>file.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:script &lt;destfilename&gt;</td>
<td>When you use this option, the copy command will not validate the downloaded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>script file. An example of the CLI command follows: (NETGEAR Switch) #copy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tftp://1.1.1.1/file.scr nvram:script file.scr</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:sshkey-dsa</td>
<td>Downloads an SSH key file. For more information, see Secure Shell (SSH)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Commands on page 601.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:sshkey-rsa1</td>
<td>Downloads an SSH key file.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:sshkey-rsa2</td>
<td>Downloads an SSH key file.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:sslpm-dhweak</td>
<td>Downloads an HTTP secure-server certificate.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:sslpm-dhstrong</td>
<td>Downloads an HTTP secure-server certificate.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:sslpm-root</td>
<td>Downloads an HTTP secure-server certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, see Hypertext Transfer Protocol (HTTP) Commands on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>page 605.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:sslpm-server</td>
<td>Downloads an HTTP secure-server certificate.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:startup-config</td>
<td>Downloads the startup configuration file to the system.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:system-image</td>
<td>Downloads a code image to the system.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>nvram:license-key</td>
<td>Download the license date to the system.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>ias-users</td>
<td>Downloads IAS users file by sftp, scp or tftp.</td>
</tr>
</tbody>
</table>
### Utility Commands

#### ProSafe Managed Switch

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;url&gt;</td>
<td>{image1</td>
<td>image2}</td>
</tr>
<tr>
<td>{image1</td>
<td>image2}</td>
<td>&lt;url&gt;</td>
</tr>
<tr>
<td>image1</td>
<td>image2</td>
<td>Copy image1 to image2.</td>
</tr>
<tr>
<td>image2</td>
<td>image1</td>
<td>Copy image2 to image1.</td>
</tr>
<tr>
<td>{image1</td>
<td>image2}</td>
<td>unit://&lt;unit&gt;/&lt;image1</td>
</tr>
<tr>
<td>{image1</td>
<td>image2}</td>
<td>unit://*/&lt;image1</td>
</tr>
</tbody>
</table>

- **write memory**

  Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running config nvram:startup-config`.

  **Format**
  
  ```
  write memory
  ```

  **Mode**
  
  Privileged EXEC

---

### Simple Network Time Protocol (SNTP) Commands

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

#### snntp 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**
  
  ```
  snntp broadcast client poll-interval <poll-interval>
  ```

- **Mode**
  
  Global Config

#### no snntp broadcast client poll-interval

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

- **Format**
  
  ```
  no snntp broadcast client poll-interval
  ```

- **Mode**
  
  Global Config

---
**sntp client mode**

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

**Default**

disabled

**Format**

`sntp client mode [broadcast | unicast]`

**Mode**

Global Config

**no sntp client mode**

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

**Format**

`no sntp client mode`

**Mode**

Global Config

**sntp client port**

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

**Default**

123

**Format**

`sntp client port <portid>`

**Mode**

Global Config

**no sntp client port**

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

**Format**

`no sntp client port`

**Mode**

Global Config

**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
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

---

**snntp unicast client poll-timeout**

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

**Default**

5

**Format**

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

**Mode**

Global Config

---

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

---

**snntp 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

---

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
**sntp server**

This command configures an SNTP server (a maximum of three). The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

**Format**

```
sntp server <ipaddress|ipv6address|hostname> [ <priority> [ <version> [ <portid> ] ] ]
```

**Mode**

Global Config

**no sntp server**

This command deletes an server from the configured SNTP servers.

**Format**

```
no sntp server remove <ipaddress|ipv6address|hostname>
```

**Mode**

Global Config

**clock timezone**

When using SNTP/NTP time servers to update the switch’s clock, the time data received from the server is based on Coordinated Universal Time (UTC) which is the same as Greenwich Mean Time (GMT). This may not be the time zone in which the switch is located. Use the **clock timezone** command to configure a time zone specifying the number of hours and optionally the number of minutes difference from UTC. To set the switch clock to UTC, use the **no** form of the command.

**Format**

```
clock timezone zone-name +/-hours-offset [+/-minutes-offset]
```

**Mode**

Global Config

**Default**

```
no clock timezone
```

- **Zone name:** A name to associate with the time zone
- **Hours-offset:** Number of hours difference with UTC
- **Minutes-offset:** Number of minutes difference with UTC

**no clock timezone**

This command sets the switch to UTC time.

**Format**

```
no clock timezone
```

**Mode**

Global Config

**clock summer-time recurring**

Use the **clock summer-time recurring** command to set the summertime offset to UTC recursively every year. If the optional parameters are not specified, they are read as either '0' or '0', as appropriate.
Use the following parameters to configure the summer-time.

- **USA**—the US Daylight saving time setting is used (Start --- March, 2nd sunday 02:00 AM, End --- Nov, 1st sunday, 2:00 AM)
- **EU**—the European Union Daylight savings time is used (Start --- March, 5th Sunday 02:00 AM, End --- October, 5th Sunday, 3:00 AM)
- **week**—Week of the month. (Range: 1-5, first, last)
- **day**—Day of the week. (Range: The first three letters by name; sun, for example.)
- **month**—Month. (Range: The first three letters by name; jan, for example.)
- **hh:mm**—Time in 24-hour format in hours and minutes. (Range: hh:0-23, mm: 0-59)
- **offset**—Number of minutes to add during the summertime. (Range: 1-1440)
- **acronym**—The acronym for the time zone to be displayed when summertime is in effect. (Range: Up to four characters)

For example:

(Switch)(Config)# clock summer-time recurring 1 sun jan 00:10 2 mon mar 10:00 offset 1 zone ABC

**clock summer-time date**

Use the **clock summer-time date** command to set the summertime offset to UTC. If the optional parameters are not specified, they are read as either '0' or '\0', as appropriate.

- **date**—Day of the month. (Range: 1-31)
- **month**—Month. (Range: The first three letters by name; jan, for example.)
- **year**—Year. (Range: 2000-2097)
- **hh:mm**—Time in 24-hour format in hours and minutes. (Range: hh: 0-23, mm: 0-59)
- **offset**—Number of minutes to add during the summertime. (Range: 1-1440)
- **acronym**—The acronym for the time zone to be displayed when summertime is in effect. (Range: Up to four characters)

For example:

(Switch)(config)# clock summer-time date 1 Apr 2007 02:00 28 Oct 2007 offset 90 zone EST
or

(Switch) (config)# clock summer-time date Apr 1 2007
02:00 Oct 28 2007 offset 90 zone EST

**no clock summer-time**

Use the **no clock summer-time** command to reset the summertime offset.

**Format**

```plaintext
no clock summer-time
```

**Mode**

Global Config

**For example:**

```plaintext
console(config)#no clock summer-time
```

**show sntp**

This command is used to display SNTP settings and status.

**Format**

```plaintext
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 Unicast</td>
<td>Time of last transmit query (in unicast mode).</td>
</tr>
<tr>
<td>Attempt Time</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>
<tr>
<td>Multicast Count</td>
<td>Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot.</td>
</tr>
</tbody>
</table>

**show sntp client**

This command is used to display SNTP client settings.

**Format**

```plaintext
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, Unicast, or Multicast).</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.</td>
</tr>
<tr>
<td>Client Mode</td>
<td>Configured SNTP Client Mode.</td>
</tr>
</tbody>
</table>

**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.</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>
<tr>
<td>Server Mode</td>
<td>SNTP Server mode.</td>
</tr>
<tr>
<td>Server Maximum Entries</td>
<td>Total number of SNTP Servers allowed.</td>
</tr>
<tr>
<td>Server Current Entries</td>
<td>Total number of SNTP configured.</td>
</tr>
</tbody>
</table>

For each configured server:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>IP address or hostname of configured SNTP Server.</td>
</tr>
<tr>
<td>Address Type</td>
<td>Address Type of configured SNTP server.</td>
</tr>
<tr>
<td>Priority</td>
<td>IP priority type of the configured server.</td>
</tr>
<tr>
<td>Version</td>
<td>SNTP Version number of the server. The protocol version used to query the server in unicast mode.</td>
</tr>
<tr>
<td>Port</td>
<td>Server Port Number.</td>
</tr>
<tr>
<td>Last Attempt Time</td>
<td>Last server attempt time for the specified server.</td>
</tr>
</tbody>
</table>
show clock

Use the show clock command in Privileged EXEC or User EXEC mode to display the time and date from the system clock. Use the show clock detail command to show the time zone and summertime configuration.

Format: `show clock [detail]`

Mode:
- User EXEC
- Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update Status</td>
<td>Last server attempt status for the server.</td>
</tr>
<tr>
<td>Total Unicast Requests</td>
<td>Number of requests to the server.</td>
</tr>
<tr>
<td>Failed Unicast Requests</td>
<td>Number of failed requests from server.</td>
</tr>
</tbody>
</table>

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.

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
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

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

no client-identifier

This command deletes the client identifier.

Format   no client-identifier
Mode     DHCP Pool Config

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

no client-name

This command removes the client name.

Format   no client-name
Mode     DHCP Pool Config
**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

**no default-router**

This command removes the default router list.

Format: no default-router

Mode: DHCP Pool Config

**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

**no dns-server**

This command removes the DNS Server list.

Format: no dns-server

Mode: DHCP Pool Config

**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
**no hardware-address**

This command removes the hardware address of the DHCP client.

**Format**

no hardware-address

**Mode**

DHCP Pool Config

**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

**no host**

This command removes the IP address of the DHCP client.

**Format**

no host

**Mode**

DHCP Pool Config

**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

**no lease**

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

**Format**

no lease

**Mode**

DHCP Pool Config
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

no network

This command removes the subnet number and mask.

Format
no network

Mode
DHCP Pool Config

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

no bootfile

This command deletes the boot image name.

Format
no bootfile

Mode
DHCP Pool Config

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
**no domain-name**

This command removes the domain name.

**Format**

```
no domain-name
```

**Mode**

DHCP Pool Config

**netbios-name-server**

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

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

**Default**

none

**Format**

```
netbios-name-server <address> [address2]...[address8]
```

**Mode**

DHCP Pool Config

**no netbios-name-server**

This command removes the NetBIOS name server list.

**Format**

```
no netbios-name-server
```

**Mode**

DHCP Pool Config

**netbios-node-type**

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

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed
- h-node—Hybrid (recommended)

**Default**

none

**Format**

```
netbios-node-type <type>
```

**Mode**

DHCP Pool Config
no netbios-node-type

This command removes the NetBIOS node Type.

Format: no netbios-node-type
Mode: DHCP Pool Config

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

no next-server

This command removes the boot server list.

Format: no next-server
Mode: DHCP Pool Config

option

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

Default: none
Format: option <code> {ascii string | hex <string1> [<string2>...] | ip <address1> [<address2>...]}</string8>
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

---

**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

---

**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

---

**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

---

**no ip dhcp ping packets**

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

**Default**

```
0
```
**service dhcp**

This command enables the DHCP server.

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

**no service dhcp**

This command disables the DHCP server.

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

**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

**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

**ip dhcp conflict logging**

This command enables conflict logging on DHCP server.

- **Default:** enabled
- **Format:** `ip dhcp conflict logging`
- **Mode:** Global Config
**no ip dhcp conflict logging**

This command disables conflict logging on DHCP server.

*Format* no ip dhcp conflict logging  
*Mode* Global Config

**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

**clear ip dhcp server statistics**

This command clears DHCP server statistics counters.

*Format* clear ip dhcp server statistics  
*Mode* Privileged EXEC

**clear ip dhcp conflict**

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts if the asterisk (*) character is used as the address parameter.

*Default* none  
*Format* clear ip dhcp conflict `<address> | *`  
*Mode* Privileged EXEC

**show ip dhcp binding**

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

*Format* show ip dhcp binding `<address>`  
*Modes*  
- Privileged EXEC  
- User EXEC
**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>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>

**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>

**show ip dhcp server statistics**

This command displays DHCP server statistics.

**Format**

```
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 DHCP OFFER messages the server sent.</td>
</tr>
<tr>
<td>DHCP ACK</td>
<td>The number of DHCP ACK messages the server sent.</td>
</tr>
<tr>
<td>DHCP NACK</td>
<td>The number of DHCP NACK messages the server sent.</td>
</tr>
</tbody>
</table>

**show ip dhcp conflict**

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

**Format**  
show ip dhcp conflict [<ip-address>]

**Modes**

- Privileged EXEC
- User EXEC

<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>

**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.

**ip domain lookup**

Use this command to enable the DNS client.

**Default** enabled

**Format** ip domain lookup

**Mode** Global Config

**no ip domain lookup**

Use this command to disable the DNS client.

**Format** no ip domain lookup

**Mode** Global Config
ip domain name

Use this command to define a default domain name that the 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.

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

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

no ip domain list

Use this command to delete a name from a list.

Format: no ip domain list <name>

Mode: Global Config

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

no ip name-server

Use this command to remove a name server.

Format no ip name-server [server-address1...server-address8]
Mode Global Config

ip host

Use this command to define static host name-to-address mapping in the host cache. <name> is host name. <ip address> is the IP address of the host.

Default none
Format ip host <name> <ipaddress>
Mode Global Config

no ip host

Use this command to remove the name-to-address mapping.

Format no ip host <name>
Mode Global Config

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. <name> is host name. <v6 address> is the IPv6 address of the host.

Default none
Format ipv6 host <name> <v6 address>
Mode Global Config

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
**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

**no ip domain retry**

Use this command to return to the default.

Format: `no ip domain retry <number>`

Mode: Global Config

**ip domain timeout**

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter `<seconds>` specifies the time, in seconds, to wait for a response to a DNS query. `<seconds>` ranges from 0 to 3600.

Default: 3

Format: `ip domain timeout <seconds>`

Mode: Global Config

**no ip domain timeout**

Use this command to return to the default setting.

Format: `no ip domain timeout <seconds>`

Mode: Global Config

**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
### show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. `<name>` ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries.

**Format**

```
show hosts [name]
```

**Mode**

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>
</tbody>
</table>

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

```
<Switch> show hosts

Host name......................... Device
Default domain................. gm.com
Default domain list............ yahoo.com, Stanford.edu, rediff.com
Domain Name lookup.............. Enabled
Number of retries............... 5
Retry timeout period.......... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19

Configured host name-to-address mapping:

<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>
```
Packet Capture Commands

Packet capture commands assist in troubleshooting protocol-related problems with the management CPU. The packets to and from the management CPU can be captured in an internally allocated buffer area for export to a PC host for protocol analysis. Public domain packet analysis tools like Ethereal can be used to decode and review the packets in detail. Capturing can be performed in a variety of modes, either transmit-side only, receive-side only, or both. The number of packets captured will depend on the size of the captured packets.

**capture transmit packet**

This command enables the capturing of transmit packets.

**Format**
capture transmit packet

**Mode**
Global Config

**no capture transmit packet**

This command disables the capturing of transmit packets.

**Format**
no capture transmit packet

**Mode**
Global Config

**capture receive packet**

This command enables the capturing of receive packets.

**Format**
capture receive packet

**Mode**
Global Config

**no capture receive packet**

This command disables the capturing of receive packets.

**Format**
no capture receive packet

**Mode**
Global Config

**capture all packets**

This command enables the capturing of receive packets.

**Format**
capture all packet

**Mode**
Global Config
**no capture all packets**

This command disables the capturing of all packets.

**Format**

```
no capture all packets
```

**Mode**

Global Config

**capture wrap**

This command enables the Buffer Wrapping configuration. Once the capture buffer is full, writes to the buffer will wrap around to allow continuous packet capture.

**Format**

```
capture wrap
```

**Mode**

Global Config

**Default**

Enabled

**show capture packets**

This command displays packets being captured from the buffer. The output of the show command can be redirected to a text file. The resultant text file can be fed to the `text2pcap` utility or the Ethereal public domain packet analyzer, which can then be translated to a cap file.

**Format**

```
show capture packets
```

**Mode**

Global Config

**Default**

Enabled

---

**Serviceability Packet Tracing Commands**

These commands improve the capability of network engineers to diagnose conditions affecting their managed switch product.

⚠️ **CAUTION:**

The output of the `debug` commands can be long and may adversely affect system performance.

**debug arp**

Use this command to enable ARP debug protocol messages.

**Default**

disabled
Utility Commands

ProSafe Managed Switch

Format: debug arp
Mode: Privileged EXEC

no debug arp

Use this command to disable ARP debug protocol messages.

Format: no debug arp
Mode: Privileged EXEC

debug auto-voip

Use this command to enable Auto VOIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Default: disabled
Format: debug auto-voip [H323|SCCP|SIP]
Mode: Privileged EXEC

no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format: no debug auto-voip
Mode: Privileged EXEC

default clear

This command disables all previously enabled "debug" traces.

Default: disabled
Format: debug clear
Mode: Privileged EXEC

default 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
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

debug dhcp packet

Use this command to display “debug” information about DHCPv4 client activities and trace DHCPv4 packets to and from the local DHCPv4 client.

Default:  disabled
Format:  debug dhcp packet [transmit | receive]
Mode:    Privileged EXEC

no debug dhcp

Use this command to disable the display of “debug” trace output for DHCPv4 client activity.

Format:  no debug dhcp packet [transmit | receive]
Mode:    Privileged EXEC

debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default:  disabled
Format:  debug dot1x
Mode:    Privileged EXEC

no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format:  no debug dot1x
Mode:    Privileged EXEC
**debug igmpsnooping packet**

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

**Default**

disabled

**Format**

d debug igmpsnooping packet

**Mode**

Privileged EXEC

**no debug igmpsnooping packet**

This command disables tracing of IGMP Snooping packets.

**Format**

no debug igmpsnooping packet

**Mode**

Privileged EXEC

**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**

d debug igmpsnooping packet transmit

**Mode**

Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116)
908 % Pkt TX - Intf: 1/0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac:
01:00:5e:00:00:01 Src_IP: 9.1.1.1 Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group:
225.0.0.1
```

The following parameters are displayed in the trace message:

<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/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>
**Utility Commands**

**ProSafe Managed Switch**

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**Group**

Multicast group address in the IGMP header.

---

**no debug igmpsnooping transmit**

This command disables tracing of transmitted IGMP snooping packets.

**Format**

no debug igmpsnooping transmit

**Mode**

Privileged EXEC

---

**debug igmpsnooping packet receive**

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

**Default**

disabled

**Format**

debug igmpsnooping packet receive

**Mode**

Privileged EXEC

A sample output of the trace message is shown below.

```<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt RX - Intf: 1/0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05 Src_IP: 11.1.1.1 Dest_IP: 225.0.0.5 Type: Membership_Query Group: 225.0.0.5 >```

The following parameters are displayed in the trace message:

<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 unit/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>

---

Utility Commands

565
no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format:    no debug igmpsnooping receive
Mode:      Privileged EXEC

depug 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

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

depug 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
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

depbug 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

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

depbug 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

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
**debug ip pimd 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 pimd packet [receive|transmit]

**Mode**  
Privileged EXEC

**no debug ip pimd packet**

Use this command to disable debug tracing of PIMDM packet reception and transmission.

**Format**  
no debug ip pimd packet [receive|transmit]

**Mode**  
Privileged EXEC

**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

**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

**debug ip vrrp**

Use this command to enable VRRP debug protocol messages.

**Default**  
disabled
Utility Commands

ProSafe Managed Switch

Format: `debug ip vrrp`
Mode: Privileged EXEC

**no debug ip vrrp**

Use this command to disable VRRP debug protocol messages.

Format: `no debug ip vrrp`
Mode: Privileged EXEC

**debug ipv6 dhcp**

Use this command to display “debug” information about DHCPv6 client activities and trace DHCPv6 packets to and from the local DHCPv6 client.

Default: disabled
Format: `debug ipv6 dhcp`
Mode: Privileged EXEC

**no ipv6 debug dhcp**

Use this command to disable the display of “debug” trace output for DHCPv6 client activity.

Format: `no debug ipv6 dhcp`
Mode: Privileged EXEC

**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

**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
**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

**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

**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

**no debug ipv6 pimdm packet**

Use this command to disable debug tracing of PIMDMv6 packet reception and transmission.

**debug ipv6 pimsr 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
Utility Commands

**ProSafe Managed Switch**

**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

**debug lacp packet**

This command enables tracing of LACP packets received and transmitted by the switch.

**Default**

disabled

**Format**

debug lacp packet

**Mode**

Privileged EXEC

A sample output of the trace message is shown below.

<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %%
Pkt TX - Intf: 1/0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key: 0x36

**no debug lacp packet**

This command disables tracing of LACP packets.

**Format**

no debug lacp packet

**Mode**

Privileged EXEC

**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.

**Default**

disabled

**Format**

debug mldsnooping packet [receive|transmit]

**Mode**

Privileged EXEC
no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

debug ospf packet

This command enables tracing of OSPF packets received and transmitted by the switch.

<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:2/0/48 Src Ip:192.168.50.2 DestIp:224.0.0.5 AreaId:0.0.0.0 Type:HELLO NetMask:255.255.255.0
     DesignRouter:0.0.0.0 Backup:0.0.0.0

<15> JAN 02 11:03:35 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25431 % Pkt TX -
     Intf:2/0/48 Src Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:DB_DSCR Mtu:1500 Options:E
     Flags: I/M/MS Seq:126166

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25434 % Pkt RX -
     Intf:2/0/48 Src Ip:192.168.50.2 DestIp:192.168.50.1 AreaId:0.0.0.0 Type:LS_REQ Length: 1500

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25435 % Pkt TX -
     Intf:2/0/48 Src Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:LS_UPD Length: 1500

<15> JAN 02 11:03:37 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25441 % Pkt TX -
     Intf:2/0/48 Src Ip: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 unit/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>Netmask</td>
<td>The netmask in the hello packet.</td>
</tr>
<tr>
<td>DesignRouter</td>
<td>Designated Router IP address.</td>
</tr>
<tr>
<td>Backup</td>
<td>Backup router IP address.</td>
</tr>
</tbody>
</table>

**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>

no debug ospf packet

This command disables tracing of OSPF packets.

Format       : no debug ospf packet
Mode         : Privileged EXEC

debug ipv6 ospfv3 packet

Use this command to enable OSPFv3 packet debug trace.

Default      : disabled
Format       : debug ipv6 ospfv3 packet
Mode         : Privileged EXEC

no debug ipv6 ospfv3 packet

Use this command to disable tracing of OSPFv3 packets.

Format       : no debug ipv6 ospfv3 packet
Mode         : Privileged EXEC

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.

Default      : disabled
Format       : debug ping packet
Mode         : Privileged EXEC

A sample output of the trace message is shown below.

<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182040176]: sim_debug.c(128) 20 % Pkt TX - Intf: 1/0/1(1), SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST

<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21 % Pkt RX - Intf: 1/0/1(1), S
ProSafe Managed Switch

RC_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 unit/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>

**no debug ping packet**

This command disables tracing of ICMP echo requests and responses.

- **Format**: no debug ping packet
- **Mode**: Privileged EXEC

**debug rip packet**

This command turns on tracing of RIP requests and responses. This command takes no options. The output is directed to the log file.

- **Default**: disabled
- **Format**: debug rip packet
- **Mode**: Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:35:15 192.168.17.29-1 RIP[181783160]: rip_map_debug.c(96) 775 %
Pkt RX on Intf: 1/0/1(1), Src_IP:43.1.1.1 Dest_IP:43.1.1.2
Rip_Version: RIPv2 Packet_Type:RIP_RESPONSE
ROUTE 1): Network: 10.1.1.0 Mask: 255.255.255.0 Metric: 1
ROUTE 2): Network: 40.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 3): Network: 10.50.50.0 Mask: 255.255.255.0 Metric: 1
ROUTE 4): Network: 41.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 5): Network:42.0.0.0 Mask:255.0.0.0 Metric:1
Another 6 routes present in packet not displayed.
```
The following parameters are displayed in the trace message:

<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 unit/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 &lt;RIPv1 or RIPv2&gt;.</td>
</tr>
<tr>
<td>Packet_Type</td>
<td>Type of RIP packet. &lt;RIP_REQUEST or RIP_RESPONSE&gt;.</td>
</tr>
<tr>
<td>Routes</td>
<td>Up to 5 routes in the packet are displayed in the following format: Network: &lt;a.b.c.d&gt; Mask &lt;a.b.c.d&gt; Next_Hop &lt;a.b.c.d&gt; Metric &lt;a&gt; The next hop is only displayed if it is different from 0.0.0.0. For RIPv1 packets, Mask is always 0.0.0.0.</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>

**no debug rip packet**

This command disables tracing of RIP requests and responses.

**Format**

no debug rip packet

**Mode**

Privileged EXEC

**debug sflow packet**

Use this command to enable sFlow debug packet trace.

**Default**

disabled

**Format**

debug sflow packet

**Mode**

Privileged EXEC

**no debug sflow packet**

Use this command to disable sFlow debug packet trace.

**Format**

no debug sflow packet

**Mode**

Privileged EXEC
**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

**no debug spanning-tree bpdu**

This command disables tracing of spanning tree BPDUs.

- **Format**: `no debug spanning-tree bpdu`
- **Mode**: Privileged EXEC

**debug spanning-tree bpdu receive**

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

- **Default**: disabled
- **Format**: `debug spanning-tree bpdu receive`
- **Mode**: Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX - Intf: 1/0/9(9), Source_Mac: 00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root Priority: 0x8000 Path Cost: 0
```

The following parameters are displayed in the trace message:

<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>
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

debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default  disabled
Format    debug spanning-tree bpdu transmit
Mode      Privileged EXEC

A sample output of the trace message is shown below.

<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s debug.c(1249) 101 % Pkt TX
- Intf: 1/0/7(7), Source_Mac: 00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00,
Root_Priority: 0x8000 Path_Cost: 0

The following parameters are displayed in the trace message:

<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>

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
Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.

**Note:** The cable test feature is supported only for copper cable. It is not supported for optical fiber cable. If the port has an active link while the cable test is run, the link can go down for the duration of the test.

cablestatus

This command returns the status of the specified port.

**Format**
cablestatus <unit/slot/port>

**Mode**
Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cable Status  | One of the following statuses is returned:  
  • Normal: The cable is working correctly.  
  • Open: The cable is disconnected or there is a faulty connector.  
  • Short: There is an electrical short in the cable.  
  • Cable Test Failed: The cable status could not be determined. The cable may in fact be working. |
| Cable Length  | If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined. |

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.
**sflow receiver**

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

**Format**

```
sflow receiver <rcvr_idx> owner <owner-string> timeout <rcvr_timeout>
max datagram <size> ip/ipv6 <ip> port <port>
```  

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver Owner</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>Receiver Timeout</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 0-4294967295 seconds. The default is zero (0).</td>
</tr>
<tr>
<td>Receiver Max Datagram Size</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>Receiver IP</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>Receiver Port</td>
<td>The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.</td>
</tr>
</tbody>
</table>

**no sflow receiver**

Use this command to set the sFlow collector parameters back to the defaults.

**Format**

```
no sflow receiver <indx> {ip <ip-address> | maxdatagram <size> | owner <string> timeout <interval> | port <14-port>}
```  

**Mode**

Global Config

**sflow sampler**

A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance for this data source if `<rcvr_idx>` is valid.

**Format**

```
sflow sampler {<rcvr-index> | rate <sampling-rate> | maxheadersize <size>}  
```  

**Mode**

Interface Config
Utility Commands

ProSafe Managed Switch

<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>

**no sflow sampler**

Use this command to reset the sFlow sampler instance to the default settings.

Format

```
no sflow sampler {<rcvr-indx> | rate <sampling-rate> | maxheadersize <size>}
```

Mode

Interface Config

**sflow poller**

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance for this data source if <rcvr_idx> is valid.

Format

```
sflow poller {<rcvr-indx> | 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>

**no sflow poller**

Use this command to reset the sFlow poller instance to the default settings.

Format

```
no sflow poller {<rcvr-indx> | interval <poll-interval>}
```

Mode

Interface Config
**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: Netgear.</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;Netgear;1.0
IP Address................................. 10.131.12.66

**show sflow pollers**

Use this command to display the sFlow polling instances created on the switch. Use “-” for range.

**Format**

show sflow pollers

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poller DataSource</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>
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>Field</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.</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 command.

```
(switch) #show sflow receivers 1
Receiver Index................................. 1
Owner String................................... 
Time out....................................... 0
IP Address.................................... 0.0.0.0
Address Type................................... 1
Port........................................... 6343
Datagram Version............................... 5
Maximum Datagram Size......................... 1400
```

show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

Format: show sflow samplers

Mode: Privileged EXEC
ProSafe Managed Switch

<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>Packet Sampling Rate</td>
<td>The statistical sampling rate for packet sampling from this source.</td>
</tr>
<tr>
<td>Max Header Size</td>
<td>The maximum number of bytes that should be copied from a sampled packet to form a flow sample.</td>
</tr>
</tbody>
</table>

**Software License Commands**

Release 9.0 allows the XSM7224S to be licensed such that this switch can configure advanced features.

The following table lists the software license matrix for the XSM7224S:

<table>
<thead>
<tr>
<th>Switch</th>
<th>IPv4 Routing</th>
<th>IPv6 Routing</th>
<th>IP Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Switches</td>
<td>Licensed</td>
<td>Licensed</td>
<td>Licensed</td>
</tr>
</tbody>
</table>

**Note:** The software license will allow the user to download a license file only on the Master unit. The file cannot be downloaded on a Slave unit.

There are two options to download the license file to the switch:

- Use the command **Copy** to download the license file through the CLI.
- Go to the **Maintenance > Download** page to download the licence file through the GUI.

**show license**

This command displays the license status.

License Date indicates the date of the license. License Status indicates whether license is active or inactive.

**Format**      show license

**Mode**        Privileged EXEC

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

(Managed Switches) #show license
License date : Apr-9-2010
License copy: 1
License Status: Active
Description: License key is active.
(Managed Switches) #

**show license features**

This command displays the features that are licensed on the switch.

**Format**
show license features

**Mode**
Privileged EXEC

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

(Managed Switches) #show license features
IGMP
MCAST
PIMDM
DVMRP
PIMSM
OSPFV3
IPV6

**IP Address Conflict Commands**

**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.

**Note:** This command takes effect only once after it is executed and cannot be saved across power cycles.

**Format**
ip address-conflict-detect run

**Mode**
Global Config
**show ip address-conflict**

This command displays the status information corresponding to the last detected address conflict.

<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>

**clear ip address-conflict-detect**

This command clears the detected address conflict status information.

**Format**

clear ip address-conflict-detect

**Mode**

Privileged EXEC

**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 blockall**

Use this command to block LLPF protocol(s) on a port. Use `blockall` to filter all PDUs with a DMAC of 01:00:00:0C:CC:CX on the interface. Use `blockisdp` to filter the ISDP packets on the interface. Use `blockvtp` to filter the VTP packets on the interface. Use `blockdtp` to filter the DTP packets on the interface. Use `blockudld` to filter the UDLD packets on the interface. Use `blockpagp` to filter the PAGP packets on the interface. Use `blocksstp` to filter the SSTP packets on the interface.

**Format**

llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall}

**Mode**

Interface Config

**Default**

Disable
**no llpf**

Use this command to unblock LLPF protocol(s) on a port.

**show llpf interface all**

Use this command to display the status of LLPF rules configured on a particular port or on all ports.

**Format**

```
show llpf interface [all | unit/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>
<tr>
<td>Block SSTP</td>
<td>Shows whether the port blocks SSTP PDUs.</td>
</tr>
<tr>
<td>Block All</td>
<td>Shows whether the port blocks all proprietary PDUs available for the LLDP feature.</td>
</tr>
</tbody>
</table>
This chapter describes the management commands available in the managed switch CLI.

This chapter contains the following sections:

- Configuring the Switch Management CPU
- Network Interface Commands
- Console Port Access Commands
- Telnet Commands
- Secure Shell (SSH) Commands
- Management Security Commands
- Hypertext Transfer Protocol (HTTP) Commands
- Access Commands
- User Account Commands
- SNMP Commands
- RADIUS Commands
- TACACS+ Commands
- Configuration Scripting Commands
- Pre-login Banner and System Prompt Commands
- Switch Database Management (SDM) Templates
- IPv6 Management Commands

The commands in this chapter are in 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.
Configuring the Switch Management CPU

To manage the switch via the web GUI or telnet, an IP address needs to be assigned to the switch management CPU. Whereas there are CLI commands that can be used to do this, ezconfig simplifies the task. The tool is applicable to all NETGEAR 7000-series managed switches, and allows you to configure the following parameters:

1. The administrator’s user password and administrator-enable password
2. Management CPU IP address and network mask
3. System name and location information

The tool is interactive and uses questions to guide you through the steps required to perform its task. At the end of the session, it will ask you if you want to save the changed information. To see exactly what has been changed by ezconfig at the end of the session, use the show running-config command.

To perform any switch configuration other than the items listed above, use other CLI commands or the Web GUI.

ezconfig

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.

<table>
<thead>
<tr>
<th>Format</th>
<th>ezconfig</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>
The following is an example of an ezconfig session.

```
NETGEAR EZ Configuration Utility
--------------------------------
Hello and Welcome!

This utility will walk you thru assigning the IP address for the switch management CPU. It will allow you to save the changes at the end. After the session, simply use the newly assigned IP address to access the Web GUI using any public domain Web browser.

Admin password not defined. Do you want to change the password? (Y/N/Q)  y
Enter new password:********
Confirm new password:********
Password Changed!

The 'enable' password required for switch configuration via the command line interface is currently not configured. Do you wish to change it (Y/N/Q)?  y
Enter new password:********
Confirm new password:********
Password Changed!

Assigning an IP address to your switch management

Current IP Address Configuration
--------------------------------
IP address: 0.0.0.0
Subnet mask: 0.0.0.0
Gateway address: 0.0.0.0

Would you like to assign an IP address now (Y/N/Q)?  y
IP Address: 10.10.10.1
Subnet mask: 255.255.255.0
Gateway address: 10.10.10.10

Do you want to assign switch name and location information (Y/N/Q)?  y
System Name: testunit1
System Location: testlab
System Contact: Bud Lightyear

There are changes detected, do you wish to save the changes permanently (Y/N)?  y

The configuration changes have been saved successfully. Please enter 'show running-config' to see the final configuration.

Thanks for using EzConfig!
```
Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see step on page 64.

**enable (Privileged EXEC access)**

Use this command to access the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

**Format**

```
enable
```

**Mode**

User EXEC

**network parms**

Use this command to set the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet.

**Format**

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

**Mode**

Privileged EXEC

**network protocol**

Use this command to specify 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

**network mac-address**

Use this command to set 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

**network mac-type**

Use this command to specify 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

**no network mac-type**

Use this command to reset the value of MAC address to its default.

**Format**

```
no network mac-type
```

**Mode**

Privileged EXEC

**network javamode**

Use this command to specify 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

**no network javamode**

Use this command to disallow 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

**show network**

Use this command to display 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 &quot;up&quot;.</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>
<tr>
<td>IPv6 Default Router</td>
<td>The IPv6 default router address.</td>
</tr>
<tr>
<td>Burned In MAC Address</td>
<td>The burned in MAC address used for in-band connectivity.</td>
</tr>
<tr>
<td>Locally Administered MAC Address</td>
<td>If desired, a locally administered MAC address can be configured for in-band connectivity. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.</td>
</tr>
<tr>
<td>MAC Address Type</td>
<td>The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.</td>
</tr>
</tbody>
</table>

The following shows example CLI display output for the network port.

(Netgear Switch) #show network

```
Interface Status......................... Always Up
IP Address................................ 10.250.3.1
Subnet Mask............................... 255.255.255.0
Default Gateway............................ 10.250.3.3
IPv6 Administrative Mode............... Enabled
IPv6 Address/Length is .................. FE80::1210:18FF:FE82:337/64
IPv6 Address/Length is .................. 3099::1/64
IPv6 Address/Length is .................. 3099::1210:18FF:FE82:337/64
```
IPv6 Default Router is ....................... FE80::204:76FF:FE73:423A
Burned In MAC Address........................ 00:10:18:82:03:37
Locally Administered MAC Address......... 00:00:00:00:00:00
MAC Address Type............................ Burned In
Network Configuration Protocol Current..... None
Management VLAN ID.......................... 1
Web Mode....................................... Enable
Java Mode...................................... Enable

**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.

*configuration*

Use this command to access Global Config mode. From Global Config mode, you can configure a variety of system settings, including user accounts. You can also enter other command modes, including Line Config mode.

**Format**

```
configuration
```

**Mode**

Privileged EXEC

*line*

Use this command to access Line Config mode, which allows you to configure various Telnet settings, ssh settings, and the console port.

**Format**

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

**Mode**

Global Config

*serial baudrate*

Use this command to specify 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
no serial baudrate

Use this command to set the communication rate of the terminal interface.

Format: no serial baudrate
Mode: Line Config

serial timeout

Use this command to specify 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

no serial timeout

Use this command to set the maximum connect time (in minutes) without console activity.

Format: no serial timeout
Mode: Line Config

login authentication

Use this command in line configuration mode to specify a login authentication method list for remote telnet or console.

Format: login authentication {default | list-name}
Mode: Line Config

no login authentication

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

Format: no login authentication {default | list-name}
Mode: Line Config
**enable authentication**

Use this command in line configuration mode to specify an authentication method list when the user accesses a higher privilege level in remote telnet or console.

**Format**

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

**Mode**

Line Config

**no enable authentication**

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

**Format**

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

**Mode**

Line Config

**show serial**

Use this command to display 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. Any numeric value between 0 and 160 is allowed, the factory default is 5. 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. The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory default is 9600 baud.</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 Type</td>
<td>The Parity Method used on the Serial Port. The Parity Method is always None.</td>
</tr>
</tbody>
</table>

**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.
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

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

telnet

Use this command to establish a new outbound Telnet connection to a remote host. The host value must be a valid IP address or host name. Valid values for port should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If [debug] is used, the current Telnet options enabled is displayed. The optional line parameter sets the outbound Telnet operational mode as ‘linemode’ where, by default, the operational mode is ‘character mode’. The noecho option disables local echo.

Format: telnet <ip-address|hostname> <port> [debug] [line] [noecho]

Modes:
- Privileged EXEC
- User EXEC

transport input telnet

Use this command to regulate new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.

---

Note: If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the ip telnet server enable command to enable Telnet Server Admin Mode.
**no transport input telnet**

Use this command to prevent new Telnet sessions from being established.

- **Format**: `no transport input telnet`
- **Mode**: Line Config

**transport output telnet**

Use this command to regulate 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

**no transport output telnet**

Use this command to prevent new outbound Telnet connection from being established.

- **Format**: `no transport output telnet`
- **Mode**: Line Config

**session-limit**

Use this command to specify 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
**no session-limit**

Use this command to set the maximum number of simultaneous outbound Telnet sessions to the default value.

**Format**

```
no session-limit
```

**Mode**

Line Config

**session-timeout**

Use this command to set the Telnet session timeout value. The timeout value unit of time is minutes.

**Default**

```
5
```

**Format**

```
session-timeout <1-160>
```

**Mode**

Line Config

**no session-timeout**

Use this command to set the Telnet session timeout value to the default. The timeout value unit of time is minutes.

**Format**

```
no session-timeout
```

**Mode**

Line Config

**telnetcon maxsessions**

Use this command to specify 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**

```
4
```

**Format**

```
telnetcon maxsessions <0-4>
```

**Mode**

Privileged EXEC

**no telnetcon maxsessions**

Use this command to set the maximum number of Telnet connection sessions that can be established to the default value.

**Format**

```
no telnetcon maxsessions
```

**Mode**

Privileged EXEC
**telnetcon timeout**

Use this command to set 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.

| Default | 5 |
| Format | `telnetcon timeout <1-160>` |
| Mode | Privileged EXEC |

**Note:** When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

**no telnetcon timeout**

Use this command to set the Telnet connection session timeout value to the default.

| Format | `no telnetcon timeout` |
| Mode | Privileged EXEC |

**show telnet**

Use this command to display 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 |
show telnetcon

Use this command to display 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</td>
<td>This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. 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>
</tbody>
</table>

Secure Shell (SSH) Commands

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

**Note:** The system allows a maximum of 5 SSH sessions.
**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

**ip ssh protocol**

Use this command to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

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

**ip ssh server enable**

Use this command to enable the IP secure shell server.

- **Default**: disabled
- **Format**: `ip ssh server enable`
- **Mode**: Privileged EXEC

**no ip ssh server enable**

Use this command to disable the IP secure shell server.

- **Format**: `no ip ssh server enable`
- **Mode**: Privileged EXEC

**sshcon maxsessions**

Use this command to specify 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
**no sshcon maxsessions**

Use this command to set the maximum number of allowed SSH connection sessions to the default value.

**Format**

```
no sshcon maxsessions
```

**Mode**

Privileged EXEC

**sshcon timeout**

Use this command to set the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

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

**Default**

Default: 5

**Format**

```
sshcon timeout <1-160>
```

**Mode**

Privileged EXEC

**no sshcon timeout**

Use this command to set the SSH connection session timeout value, in minutes, to the default.

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

**Format**

```
no sshcon timeout
```

**Mode**

Privileged EXEC

**show ip ssh**

Use this command to display 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>
</tbody>
</table>
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.

**crypto certificate generate**

Use this command to generate self-signed certificate for HTTPS. The generate RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format  
crypto certificate generate
Mode     Global Config

**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

**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
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

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

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

Hypertext Transfer Protocol (HTTP) Commands

This section describes the commands you use to configure 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.

ip http server

Use this command to enable 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
**no ip http server**

Use this command to disable access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

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

**ip http secure-server**

Use this command to enable the secure socket layer for secure HTTP.

<table>
<thead>
<tr>
<th>Default</th>
<th>disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip http secure-server</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

**no ip http secure-server**

Use this command to disable the secure socket layer for secure HTTP.

<table>
<thead>
<tr>
<th>Format</th>
<th>no ip http secure-server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

**ip http java**

Use this command to enable the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

<table>
<thead>
<tr>
<th>Default</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>ip http java</td>
</tr>
<tr>
<td>Mode</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

**no ip http java**

Use this command to disable the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

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

**ip http session hard-timeout**

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

Default  24
Format    ip http session hard-timeout <0-168>
Mode      Privileged EXEC

**no ip http session hard-timeout**

Use this command to restore the hard timeout for un-secure HTTP sessions to the default value.

Format    no ip http session hard-timeout
Mode      Privileged EXEC

**ip http authentication**

Use this command to specify the authentication methods for http server users. 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 specified as an authentication method after radius, no authentication is used if the radius server is down.

Format    ip http authentication method1 [method2 ...]
Mode      Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Uses the local username database for 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>
<tr>
<td>None</td>
<td>Uses no authentication.</td>
</tr>
</tbody>
</table>

**no ip http authentication**

Use this command to restore the authentication methods to the default.

Format    no ip http authentication method1 [method2 ...]
Mode      Global Config
ip http session maxsessions

Use this command to limit the number of allowable un-secure HTTP sessions. Zero is the configurable minimum.

Default: 16
Format: ip http session maxsessions <0-16>
Mode: Privileged EXEC

no ip http session maxsessions

Use this command to restore the number of allowable un-secure HTTP sessions to the default value.

Format: no ip http session maxsessions
Mode: Privileged EXEC

ip http session soft-timeout

Use this command to configure the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch.

Default: 5
Format: ip http session soft-timeout <0-60>
Mode: Privileged EXEC

no ip http session soft-timeout

Use this command to reset the soft timeout for un-secure HTTP sessions to the default value.

Format: no ip http session soft-timeout
Mode: Privileged EXEC

ip http secure-session maxsessions

Use this command to limit the number of secure HTTP sessions. Zero is the configurable minimum.

Default: 16
Format: ip http secure-session maxsessions <0-16>
Mode: Privileged EXEC
no ip http secure-session maxsessions

Use this command to restore the number of allowable secure HTTP sessions to the default value.

Format no ip http secure-session maxsessions
Mode Privileged EXEC

ip http secure-session soft-timeout

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

Default 5
Format ip http secure-session soft-timeout <1-60>
Mode Privileged EXEC

no ip http secure-session soft-timeout

Use this command to restore the soft timeout for secure HTTP sessions to the default value.

Format no ip http secure-session soft-timeout
Mode Privileged EXEC

ip http secure-session hard-timeout

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

Default 24
Format ip http secure-session hard-timeout <1-168>
Mode Privileged EXEC

no ip http secure-session hard-timeout

Use this command to reset the hard timeout for secure HTTP sessions to the default value.

Format no ip http secure-session hard-timeout
Mode Privileged EXEC
**ip https authentication**

Use this command to specify the authentication methods for http server users. 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. If `none` is specified as an authentication method after `radius`, no authentication is used if the radius server is down.

**Format**

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

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Uses the local username database for 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>
<tr>
<td>None</td>
<td>Uses no authentication.</td>
</tr>
</tbody>
</table>

**no ip https authentication**

Use this command to restore the authentication methods to the default for http server users.

**Format**

```
no ip https authentication method1 [method2 ...]
```

**Mode**

Global Config

**ip http secure-port**

Use this command to set the SSL port where port can be 1-65535 and the default is port 443.

**Default**

443

**Format**

```
ip http secure-port <portid>
```

**Mode**

Privileged EXEC

**no ip http secure-port**

Use this command to reset the SSL port to the default value.

**Format**

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

**Mode**

Privileged EXEC
**ip http secure-protocol**

Use this command 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

**show ip http**

Use this command to display 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>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 TSL1.</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>
## Access Commands

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

### 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.

**Format**

```
disconnect {<session_id> | all}
```

**Mode**

Privileged EXEC

### show loginsession

Use this command to display current Telnet and serial port connections to the switch.

**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 EIA-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>

## User Account Commands

This section describes the commands you use to add, manage, and delete system users. The 7000 series software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

**Note:** You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.
**username**

Use this command 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> [level level] [encrypted]
[overridecomplexity-check]
```

**Mode**

Global Config

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the user, up to 32 characters.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the users 8-64 characters. This value can be zero if the no passwords min-length command has been executed. The special characters allowed in the password include: ! # $ &amp; ' ( ) ^ * + , - / : ; &lt; = &gt; @ [ \ ] _ ` {</td>
</tr>
<tr>
<td>level</td>
<td>Specifies the user level. If not specified, the privilege level is 1. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15. Enter access level 1 for Read Access or 15 for Read/Write Access.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypted password you enter, copied from another device configuration.</td>
</tr>
<tr>
<td>override-complexity-check</td>
<td>Disables the validation of the password strength.</td>
</tr>
</tbody>
</table>

**no username**

Use this command to remove a user account.

**Format**

```
no username <username>
```

**Mode**

Global Config

---

**Note:** You cannot delete the “admin” user account.

**username nopassword**

Use this command to remove the password from a user.

**Format**

```
username <name> nopassword [level level]
```

**Mode**

Global Config
**username <username> unlock**

Use this command to unlock a user’s account. Only a user with read/write access can re-activate a locked user account.

**Format**
```plaintext
username <username> unlock
```

**Mode**
Global Config

**username snmpv3 accessmode**

Use this command to specify 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**
```plaintext
username snmpv3 accessmode <username> {readonly | readwrite}
```

**Mode**
Global Config

**no username snmpv3 accessmode**

Use this command to set 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**
```plaintext
no username snmpv3 accessmode <username>
```

**Mode**
Global Config

**username snmpv3 authentication**

Use this command to specify 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**
```plaintext
username snmpv3 authentication <username> {none | md5 | sha}
```

**Mode**
Global Config
no username snmpv3 authentication

Use this command to set 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

username snmpv3 encryption

Use this command to specify 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

no username snmpv3 encryption

Use this command to set 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

show users

Use this command to display the configured user names and their settings. This command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format  show users
Mode    Privileged EXEC
show users accounts

Use this command to display the local user status with respect to user account lockout and password aging.

Format show users accounts
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>Privilege</td>
<td>The user’s privilege level (1-15).</td>
</tr>
<tr>
<td>Password aging</td>
<td>The password aging time for the local users.</td>
</tr>
<tr>
<td>Lockout Status</td>
<td>Indicates whether the user account is locked out (true or false).</td>
</tr>
<tr>
<td>Password Expiration Date</td>
<td>The current password expiration date in date format.</td>
</tr>
</tbody>
</table>

show users accounts detail

This command displays the local user status with respect to user account lockout and password aging. It also includes information about Password strength and complexity.

Format show users accounts detail
Mode Privileged EXEC

(Switch) #show users accounts detail
UserName................................. admin
Privilege........................................ 15
Password Aging............................... ---
Password Expiry............................... ---
show users long

Use this command to display the user’s full name.

Format: show users long
Mode: Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The full name of the user.</td>
</tr>
</tbody>
</table>

show users login-history

Use this command to display the users who have logged in previously.

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Time</td>
<td>The time at which the user logged in.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name used to login.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol that the user used to login.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the user.</td>
</tr>
</tbody>
</table>

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 0-64.

Default: 8
Format: passwords min-length <0-64>
Mode: Global Config
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

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

no passwords history

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

Format       no passwords history
Mode         Global Config

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

no passwords aging

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

Format       no passwords aging
Mode         Global Config
**passwords lock-out**

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can re-activate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

**Format**

```
passwords lock-out <1-5>
```

**Mode**

Global Config

**Default**

0

**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

**passwords strength-check**

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

**Format**

```
passwords strength-check
```

**Mode**

Global Config

**Default**

Disable

**no passwords strength-check**

Use this command to disable the password strength-check.

**Format**

```
no passwords strength-check
```

**Mode**

Global Config

**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.

**Format**

```
passwords strength minimum uppercase-letters
```

**Mode**

Global Config

**Default**

2
**no passwords strength minimum uppercase-letters**

Use this command to reset the minimum number of uppercase letters to the default value.

**Format**
no passwords strength minimum uppercase-characters

**Mode**
Global Config

**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.

**Format**
passwords strength minimum lowercase-letters

**Mode**
Global Config

**Default**
2

**no passwords strength minimum lowercase-letters**

Use this command to reset the minimum number of lowercase letters to the default value.

**Format**
no passwords strength minimum lowercase-characters

**Mode**
Global Config

**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.

**Format**
passwords strength minimum numeric-letters

**Mode**
Global Config

**Default**
2

**no passwords strength minimum numeric-characters**

Use this command to reset the minimum number of numeric characters to the default value.

**Format**
no passwords strength minimum numeric-characters

**Mode**
Global Config
**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.

**Format**

```
passwords strength minimum special-characters
```

**Mode**

Global Config

**Default**

2

**no passwords strength minimum special-characters**

Use this command to reset the minimum number of special letters to the default value.

**Format**

```
no passwords strength minimum special-characters
```

**Mode**

Global Config

**passwords strength maximum consecutive-characters**

Use this command to enforce a maximum number of consecutive characters that a password should contain. An example of consecutive characters is abcd. The valid range is 0-16. If a password has consecutive characters more than the configured limit, it fails to configure. The default is 0. A maximum of 0 means no restriction on that set of characters.

**Format**

```
passwords strength maximum consecutive-characters
```

**Mode**

Global Config

**Default**

0

**no passwords strength maximum consecutive-characters**

Use this command to reset the maximum number of consecutive characters to the default value.

**Format**

```
no passwords strength maximum consecutive-characters
```

**Mode**

Global Config

**passwords strength maximum repeated-characters**

Use this command to enforce a maximum number of repeated characters that a password should contain. An example of repeated characters is aaaa. The valid range is 0-16. If a password has a repetition of characters more than the configured limit, it fails to configure. The default is 0. A maximum of 0 means no restriction on that set of characters.

**Format**

```
passwords strength maximum repeated-characters
```

**Mode**

Global Config
Mode: Global Config

Default: 0

**no passwords strength maximum repeated-characters**

Use this command to reset the maximum number of repeated-characters to the default value.

Format: `no passwords strength maximum repeated-characters`

Mode: Global Config

**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.

Format: `passwords strength minimum character-classes`

Mode: Global Config

Default: 4

**no passwords strength minimum character-classes**

Use this command to reset the minimum number of character classes to the default value.

Format: `no passwords strength minimum character-classes`

Mode: Global Config

**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

**no passwords strength exclude-keyword**

Use this command to remove the exclude-keyword.

Format: `no passwords strength exclude-keyword`

Mode: Global Config
**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>

**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>
aaa authentication login

Use this command to set authentication at login. The default and optional list names that you create with the `aaa authentication login` command are used with the `login` authentication command. Create a list by entering the `aaa authentication login list-name method` command for a particular protocol, where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries, in the given sequence. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

An example of a method that returns an error is if a RADIUS server is not present, and an example of a method failing is when a RADIUS server cannot authenticate the client. If 'local' method is listed first, since local authentication is always available, it only has the fail condition, not error. As such, if 'local' method is the first in the list, no other method will be tried.

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.

Format

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

Mode

Global Config

Default

Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.

`list-name`  Character string used to name the list of authentication methods activated when a user logs in. Up to 12 characters.

`method1 [method2...]`  At least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password for authentication.</td>
</tr>
<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>

**Note:** The local user database is checked. This has the same effect as the following command: `aaa authentication login local`
no aaa authentication login

Use this command to remove authentication at login.

**Format**

no aaa authentication login {default | list-name}

**Mode**

Global Config

**aaa authentication enable**

Use this command to set authentication when the user access higher privilege level, use the aaa authentication enable default command in global configuration mode. The default and optional list names that you create with the aaa authentication enable command are used with the enable authentication command.

Create a list by entering the aaa authentication enable list-name method command where list-name is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. For example, if none is specified as an authentication method after radius, no authentication is used if the radius server is down. All aaa authentication enable default requests sent by the switch to a RADIUS or TACACS server include the username "$enabx.$", where x is the requested privilege level.

**Format**

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

**Mode**

Global Config

**Default**

Uses the listed authentication methods that follow this argument as the default list of methods when a user accesses a higher privilege level.

**list-name**

Character string used to name the list of authentication methods activated when a user accesses a higher privilege level. Up to 12 characters.

**method1 [method2...]**

At least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Uses the enable password for authentication.</td>
</tr>
<tr>
<td>line</td>
<td>Uses the line password 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. Uses username &quot;$enabx.$&quot;, where x is the requested privilege level.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Uses the list of all TACACS servers for authentication. Uses username &quot;$enabx.$&quot;, where x is the requested privilege level.</td>
</tr>
</tbody>
</table>
**Note:** If the default list is not set, only the enable password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway. This has the same effect as the following command:

```
aaa authentication enable default enable none
```

---

**no aaa authentication enable**

Use this command to remove the authentication method.

**Format**

```
no aaa authentication enable {default | list-name} method1 [method2...]
```

**Mode**

Global Config

**aaa authentication dot1x**

Use this command to set authentication for dot1x users. 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.

**Format**

```
aaa authentication dot1x default method1 [method2...]
```

**Mode**

Global Config

```
method1 [method2...]
```

At least one from the following table:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>local</code></td>
<td>Uses the local username database for authentication.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Uses no authentication.</td>
</tr>
<tr>
<td><code>radius</code></td>
<td>Uses the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td><code>ias</code></td>
<td>Uses the internal authentication server users database for authentication.</td>
</tr>
</tbody>
</table>
no aaa authentication dot1x

Use this command to remove the authentication at login.

Format: no aaa authentication dot1x default
Mode: Global Config

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 this command to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format: aaa ias-username <user>
Mode: Global Config

no aaa ias-user username

Use this command to remove an ias user.

Format: no aaa ias-username <user>
Mode: Global Config

password (AAA IAS User Configuration)

Use this command to specify a password for a user in the IAS database.

Format: password <password> [encrypted]
Mode: AAA IAS User 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.</td>
</tr>
</tbody>
</table>

no password(AAA IAS User Configuration)

Use this command to remove a password for a user in the IAS database.

Format: no password
Mode: AAA IAS User Config
clear aaa ias-users

Use this command to remove all users from the IAS database.

Format: clear aaa ias-users

Mode: Privileged EXEC

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

Mode: Privileged EXEC

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.

snmp-server

Use this command to set the name and the physical location of the switch and the organization responsible for the network. The range for <name>, <loc> and <con> is from 1 to 31 alphanumeric characters.

Default: none

Format: snmp-server {sysname <name> | location <loc> | contact <con>}

Mode: Global Config

snmp-server community

Use this command to add (and name) a new SNMP community. A community <name> is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of <name> can be up to 16 case-sensitive characters.

Note: Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.
Default

- Public and private, which you can rename.
- Default values for the remaining four community names are blank.

**Format**

```
no snmp-server community
```

**Mode**

Global Config

**no snmp-server community**

Use this command to remove this community name from the table. The `<name>` is the community name to be deleted.

**Format**

```
no snmp-server community <name>
```

**Mode**

Global Config

**snmp-server community ipaddr**

Use this command to set a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

**Default**

0.0.0.0

**Format**

```
snmp-server community ipaddr <ipaddr> <name>
```

**Mode**

Global Config

**no snmp-server community ipaddr**

Use this command to set a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

**Format**

```
no snmp-server community ipaddr <name>
```

**Mode**

Global Config

**snmp-server community ipmask**

Use this command to set a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one
station, and will use that machine’s IP address for the client IP address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

**Default**

0.0.0.0

**Format**

`snmp-server community ipmask <ipmask> <name>`

**Mode**

Global Config

**no snmp-server community ipmask**

Use this command to set a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

**Format**

`no snmp-server community ipmask <name>`

**Mode**

Global Config

**snmp-server community mode**

Use this command to activate an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

**Default**

• private and public communities - enabled
• other four - disabled

**Format**

`snmp-server community mode <name>`

**Mode**

Global Config

**no snmp-server community mode**

Use this command to deactivate an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

**Format**

`no snmp-server community mode <name>`

**Mode**

Global Config
**snmp-server community ro**

Use this command to restrict access to switch information. The access mode is read-only (also called public).

**Format**

```
snmp-server community ro <name>
```

**Mode**

Global Config

**snmp-server community rw**

Use this command to restrict access to switch information. The access mode is read/write (also called private).

**Format**

```
snmp-server community rw <name>
```

**Mode**

Global Config

**snmp-server enable traps violation**

Use this command to enable sending new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

**Note:** For other port security commands, see *Protected Ports Commands* on page 81.

**Default**

disabled

**Format**

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

**Mode**

Interface Config

**no snmp-server enable traps violation**

Use this command to disable sending new violation traps.

**Format**

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

**Mode**

Interface Config

**snmp-server enable traps**

Use this command to enable the Authentication Flag.

**Default**

enabled
Format: `no snmp-server enable traps`
Mode: Global Config

**no snmp-server enable traps**

Use this command to disable the Authentication Flag.

Format: `no snmp-server enable traps`
Mode: Global Config

**Note:** This command may not be available on all platforms.

**snmp-server enable traps linkmode**

Use this command to enable 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. For more information, see `snmp trap link-status` on page 635

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

**no snmp-server enable traps linkmode**

Use this command to disable Link Up/Down traps for the entire switch.

Format: `no snmp-server enable traps linkmode`
Mode: Global Config

**snmp-server enable traps multiusers**

Use this command to enable 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
no snmp-server enable traps multiusers

Use this command to disable Multiple User traps.

Format
no snmp-server enable traps multiusers

Mode
Global Config

snmp-server enable traps stpmode

Use this command to enable sending new root traps and topology change notification traps.

Default
enabled

Format
snmp-server enable traps stpmode

Mode
Global Config

no snmp-server enable traps stpmode

Use this command to disable sending new root traps and topology change notification traps.

Format
no snmp-server enable traps stpmode

Mode
Global Config

snmptrap

Use this command to add an SNMP trap receiver. The maximum length of <name> is 16 case-sensitive alphanumeric characters. The <snmpversion> is the version of SNMP. The version parameter options are snmpv1 or snmpv2. The SNMP trap address can be set using both an IPv4 address format as well as an IPv6 global address format.

The following shows an example of the CLI command.

(Netgear Switch)# snmptrap mytrap ip6addr 3099::2

---

Note: The <name> parameter does not need to be unique, however; the <name> and <ipaddr | hostname> pair must be unique. Multiple entries can exist with the same <name>, as long as they are associated with a different <ipaddr | hostname>. The reverse scenario is also acceptable. The <name> is the community name used when sending the trap to the receiver, but the <name> is not directly associated with the SNMP Community Table, See “snmp-server community” on page39.”

---
Management Commands

ProSafe Managed Switch

no snmptrap

Use this command to delete trap receivers for a community.

Format
no snmptrap <name> {ipaddr <ipaddr|hostname> | ip6addr <ip6addr|hostname}> 

Mode
Global Config

snmptrap snmpversion

Use this command to modify the SNMP version of a trap. The maximum length of <name> is 16 case-sensitive alphanumeric characters. The <snmpversion> parameter options are snmpv1 or snmpv2.

---

Note: This command does not support a “no” form.

---

snmptrap ipaddr

Use this command to assign an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

---

Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.
**snmptrap mode**

Use this command to activate or deactivate an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

**Format**

```
snmptrap mode <name> { <ipaddr | hostname> |<ip6addr |hostname>}
```

**Mode**  
Global Config

**no snmptrap mode**

Use this command to deactivate an SNMP trap. Disabled trap receivers are unable to receive traps.

**Format**

```
no snmptrap mode <name> { <ipaddr | hostname> |<ip6addr |hostname>}
```

**Mode**  
Global Config

**snmp trap link-status**

Use this command to enable link status traps by interface.

---

**Note:** This command is valid only when the Link Up/Down Flag is enabled.  
For more information, see `snmp-server enable traps linkmode` on page 632.

---

**Format**

```
snmp trap link-status
```

**Mode**  
Interface Config

**no snmp trap link-status**

Use this command to disable link status traps by interface.

---

**Note:** This command is valid only when the Link Up/Down Flag is enabled.
**Format**

no snmp trap link-status

**Mode**

Interface Config

---

**snmp trap link-status all**

Use this command to enable link status traps for all interfaces.

**Note:** This command is valid only when the Link Up/Down Flag is enabled. For more information, see `snmp-server enable traps linkmode` on page 632.

---

**Format**

snmp trap link-status all

**Mode**

Global Config

---

**no snmp trap link-status all**

Use this command to disable link status traps for all interfaces.

**Note:** This command is valid only when the Link Up/Down Flag is enabled. For more information, see `snmp-server enable traps linkmode` on page 632.

---

**Format**

no snmp trap link-status all

**Mode**

Global Config

---

**show snmpcommunity**

Use this command to display SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Versions 1, 2 or 3. For more information about the SNMP specification, see the SNMP RFCs. The SNMP agent sends traps through
TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format
show snmpcommunity

Mode
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Community Name</td>
<td>The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP address. Note: If the Subnet Mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.</td>
</tr>
<tr>
<td>Client IP Mask</td>
<td>A mask to be ANDed with the requesting entity's IP address before comparison with IP address. If the result matches with IP address then the address is an authenticated IP address. For example, if the IP address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.</td>
</tr>
<tr>
<td>Access Mode</td>
<td>The access level for this community string.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of this community access entry.</td>
</tr>
</tbody>
</table>

show snmptrap

Use this command to display SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format
show snmptrap

Mode
Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap Name</td>
<td>The community string of the SNMP trap packet sent to the trap manager. The string is case sensitive and can be up to 16 alphanumeric characters.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 address to receive SNMP traps from this device.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address to receive SNMP traps from this device.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>SNMPv2</td>
</tr>
<tr>
<td>Status</td>
<td>The receiver's status (enabled or disabled).</td>
</tr>
</tbody>
</table>

The following shows an example of the CLI command.

(Netgear Switch)#show snmptrap
show trapflags

Use this command to display 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>
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.

**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

**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

**radius accounting mode**

Use this command to enable the RADIUS accounting function.

- **Default**: disabled
- **Format**: radius accounting mode
- **Mode**: Global Config

**no radius accounting mode**

Use this command to set the RADIUS accounting function to the default value (disabled).

- **Format**: no radius accounting mode
- **Mode**: Global Config

**radius server attribute**

Use this command to specify the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the
RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format    radius server attribute <4> [ipaddr]
Mode      Global Config

<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>
</tbody>
</table>

**no radius server attribute**

Use the `no` version of this command to disable the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format    no radius server attribute <4> [ipaddr]
Mode      Global Config

The following shows an example of the command.

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

**radius server host**

Use this command to configure the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the ‘Default_RADIUS_Auth_Server’ and ‘Default_RADIUS_Acct_Server’ as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the `<auth>` parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the “no” form of the command. If you use the optional `<port>` parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The `<port>` number range is 1 - 65535, with 1812 being the default value.
**Note:** To re-configure a RADIUS authentication server to use the default UDP `<port>`, set the `<port>` parameter to 1812.

If you use the `<acct>` token, the command configures the IP address or hostname to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the “no” form of the command to remove it from the configuration. The IP address or hostname you specify must match that of a previously configured accounting server. If you use the optional `<port>` parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a `<port>` is already configured for the accounting server, the new `<port>` replaces the previously configured `<port>`. The `<port>` must be a value in the range 0 - 65535, with 1813 being the default.

**Note:** To re-configure a RADIUS accounting server to use the default UDP `<port>`, set the `<port>` parameter to 1813.

**Format**
```
radius server host {auth | acct} {<ipaddr|dnsname>} [name <servername>] [port <0-65535>] [server-type]
```

**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>

**no radius server host**

Use the `no` version of this command to delete 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

The following shows an example of the command.

```
(Switch) (Config) #radius server host acct 192.168.37.60
(Switch) (Config) #radius server host acct 192.168.37.60 port 1813
(Switch) (Config) #radius server host auth 192.168.37.60 name Network1_RADIUS_Auth_Server port 1813
(Switch) (Config) #radius server host acct 192.168.37.60 name Network2_RADIUS_Auth_Server
(Switch) (Config) #no radius server host acct 192.168.37.60
```

**radius server key**

Use this command to configure the key to be used in RADIUS client communication with the specified server. Depending on whether the 'auth' or 'acct' token is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports Radius server’s secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command’s display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

---

**Note:** The secret must be an alphanumeric value not exceeding 16 characters.

**Format**

```
radius server key {auth | acct} {<ipaddr|dnsname>} encrypted <password>
```

**Mode**

Global Config

<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>
The following shows an example of the CLI command.
```
radius server key acct 10.240.4.10 encrypted <encrypt-string>
```

**radius server msgauth**

Use this command to enable the message authenticator attribute to be used for the specified RADIUS Authenticating server.

**Format**
```
radius server msgauth <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 server.</td>
</tr>
<tr>
<td>dnsname</td>
<td>The DNS name of the server.</td>
</tr>
</tbody>
</table>

**no radius server msgauth**

Use the `no` version of this command to disable the message authenticator attribute to be used for the specified RADIUS Authenticating server.

**Format**
```
no radius server msgauth <ipaddr|dnsname>
```

**Mode**
Global Config

**radius server primary**

Use this command to designate a configured server as the primary server in the group of servers that 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>
**radius server retransmit**

Use this command to configure 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>

**no radius server retransmit**

Use this command to set the value of this global parameter to the default value.

Format: `no radius server retransmit`

Mode: Global Config

**radius server timeout**

Use this command to configure 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 &lt;1-30&gt;.</td>
</tr>
</tbody>
</table>

**no radius server timeout**

Use this command to set the timeout global parameter to the default value.

Format: `no radius server timeout`

Mode: Global Config
**show radius**

Use this command to display 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 re-transmissions.</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>

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
```
**show radius servers**

Use this command to display 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 <strong>&quot;</strong> 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>The IP address of the currently active authenticating server.</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>Number of Retransmits</td>
<td>The configured value of the maximum number of times a request packet is retransmitted.</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>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 NAS-IP-Address attribute used in RADIUS requests.</td>
</tr>
</tbody>
</table>

The following shows example CLI display output for the command.

```
(Switch) #show radius servers

Current Host Address                  Server Name                  Port  Type
------------------------------------------------------------------------------
```

Management Commands

646
(Switch) #show radius servers name

Current Host Address   Server Name                       Type
------------------------ --------------------------------- ----------
192.168.37.200          Network1_RADIUS_Server            1813  Primary
192.168.37.201          Network2_RADIUS_Server            1813  Secondary
192.168.37.202          Network3_RADIUS_Server            1813  Primary
192.168.37.203          Network4_RADIUS_Server            1813  Secondary

(Switch) #show radius servers name Default_RADIUS_Server

Server Name............................ Default_RADIUS_Server
Host Address........................... 192.168.37.58
Secret Configured...................... No
Message Authenticator ................. Enable
Number of Retransmits.................. 4
Time Duration.......................... 10
RADIUS Accounting Mode................. Disable
RADIUS Attribute 4 Mode................ Enable
RADIUS Attribute 4 Value .............. 192.168.37.60

(Switch) #show radius servers 192.168.37.58

Server Name............................ Default_RADIUS_Server
Host Address........................... 192.168.37.58
Secret Configured...................... No
Message Authenticator ................. Enable
Number of Retransmits.................. 4
Time Duration.......................... 10
RADIUS Accounting Mode................. Disable
RADIUS Attribute 4 Mode................ Enable
RADIUS Attribute 4 Value .............. 192.168.37.60

**show radius accounting**

Use this command to display a summary of configured RADIUS accounting servers.

**Format**

```
show radius accounting name [<servername>]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Field</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 Mode</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.

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

**show radius accounting statistics**

Use this command to display 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>
</tbody>
</table>
The following shows example CLI display output for the command.

(Switch) #show radius accounting statistics 192.168.37.200

RADIUS Accounting Server Name.................... Default_RADIUS_Server
Host Address........................................ 192.168.37.200
Round Trip Time..................................... 0.00
Requests............................................. 0
Retransmissions..................................... 0
Responses............................................ 0
Malformed Responses............................... 0
Bad Authenticators.................................. 0
Pending Requests.................................... 0
Timeouts.............................................. 0
Unknown Types....................................... 0
Packets Dropped..................................... 0

(Switch) #show radius accounting statistics name Default_RADIUS_Server

RADIUS Accounting Server Name.................... Default_RADIUS_Server
Host Address................................. 192.168.37.200
Round Trip Time........................... 0.00
Requests..................................... 0
Retransmissions............................ 0
Responses................................. 0
Malformed Responses........................ 0
Bad Authenticators........................ 0
Pending Requests.......................... 0
Timeouts.................................... 0
Unknown Types............................. 0
Packets Dropped............................ 0

show radius statistics

Use this command to display 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>
**ProSafe Managed Switch**

The following shows example CLI display output for the command.

```
(Switch) #show radius statistics 192.168.37.200
RADIUS Server Name............................ Default_RADIUS_Server
Server Host Address........................... 192.168.37.200
Access Requests............................... 0.00
Access Retransmissions....................... 0
Access Accepts................................ 0
Access Rejects................................ 0
Access Challenges............................ 0
Malformed Access Responses.................... 0
Bad Authenticators............................ 0
Pending Requests.............................. 0
Timeouts...................................... 0
Unknown Types................................. 0
Packets Dropped............................... 0

(Switch) #show radius statistics name Default_RADIUS_Server
RADIUS Server Name............................ Default_RADIUS_Server
Server Host Address........................... 192.168.37.200
Access Requests............................... 0.00
Access Retransmissions....................... 0
Access Accepts................................ 0
Access Rejects................................ 0
Access Challenges............................ 0
Malformed Access Responses.................... 0
Bad Authenticators............................ 0
Pending Requests.............................. 0
Timeouts...................................... 0
Unknown Types................................. 0
Packets Dropped............................... 0
```

### Table

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>The number of authentication timeouts to this server.</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>The number of packets of unknown type that were received from this server on the authentication port.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.</td>
</tr>
</tbody>
</table>

**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.

**tacacs-server host**

Use the `tacacs-server host` command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The `<ip-address|hostname>` parameter is the IP address or hostname of the TACACS+ server. To specify multiple hosts, multiple `tacacs-server host` commands can be used.

| Format       | tacacs-server host <ip-address|hostname> |
|--------------|-----------------------------|
| Mode         | Global Config               |

**no tacacs-server host**

Use the `no tacacs-server host` command to delete the specified hostname or IP address. The `<ip-address|hostname>` parameter is the IP address of the TACACS+ server.

| Format       | no tacacs-server host <ip-address|hostname> |
|--------------|-----------------------------|
| Mode         | Global Config               |

**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               |

**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

**tacacs-server timeout**

Use the `tacacs-server timeout` command to set the timeout value for communication with the TACACS+ servers. The `<timeout>` parameter has a range of 1-30 and is the timeout value in seconds.

**Default**  
5

**Format**  
tacacs-server timeout <timeout>

**Mode**  
Global Config

**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

**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
**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

**priority**

Use the `priority` command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The `<priority>` parameter specifies the priority for servers. The highest priority is 0 (zero), and the range is 0 - 65535.

- **Default**: 0
- **Format**: `priority <priority>`
- **Mode**: TACACS Config

**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

**show tacacs**

Use the `show tacacs` command to display the configuration and statistics of a TACACS+ server.

- **Format**: `show tacacs [<ip-address|hostname>]`
- **Mode**: Privileged EXEC

<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>
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 513) to capture the running configuration into a script. Use the `copy` command (see `copy` on page 534) to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- Script files are not distributed across the stack, and only live in the unit that is the master unit at the time of the file download.
- The file extension must be “.scr”.
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the “!” character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access
show telnet !Displays the information about remote connections
! Display information about direct connections
show serial
! End of the script file!
```

**Note:** To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user `jane` from a blank password to `hello`, the script entry is as follows:

```
users passwd jane " "
```
**script apply**

Use this command to apply 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

**script delete**

Use this command to delete 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

**script list**

Use this command to list all scripts present on the switch as well as the remaining available space.

**Format**  
script list

**Mode**  
Global Config

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

**script show**

Use this command to display 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>line <code>&lt;number&gt;</code>: <code>&lt;line contents&gt;</code></td>
</tr>
</tbody>
</table>
**script validate**

Use this command to validate 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

---

**Pre-login Banner and System Prompt Commands**

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

**copy (pre-login banner)**

Use a `copy` command option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using TFTP, Xmodem, Ymodem, or Zmodem.

---

**Note:** `<ip6address>` is also a valid parameter for routing packages that support IPv6.

**Default**

none

**Format**

```
copy <Code Sample Variable><tftp://<ipaddr>/<filepath>/<filename>><Code Sample Variable>
```

**Mode**

Privileged EXEC

**set prompt**

Use this command to change the name of the prompt. The length of name may be up to 64 alphanumeric characters.

**Format**

```
set prompt <prompt_string>
```

**Mode**

Privileged EXEC
Switch Database Management (SDM) Templates

You can use SDM templates to configure system resources in the switch and optimize support for specific features depending on how the switch is used in the network. You can select a template to provide the maximum system usage for a specific function. For example, you could use a routing template to optimize resources for IPv4 routing if the network environment does not use IPv6 routing.

Note the following:

- If you configure an SDM template, you must reload the switch for the configuration to take effect.
- If you try to configure IPv6 routing without first selecting the dual IPv4-IPv6 routing template, a warning message appears.

**sdm prefer**

Use this command to specify the SDM template to use on the switch.

<table>
<thead>
<tr>
<th>Default</th>
<th>ipv4-routing for IPv4 only builds, dual-ipv4-ipv6 for IPv6 builds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>sdm prefer {ipv4-routing {default</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>ipv4-routing</td>
<td>Supports IPv4 routing only.</td>
</tr>
<tr>
<td></td>
<td>- data-center: Support more ECMP next hops in IPv4 routes.</td>
</tr>
<tr>
<td></td>
<td>- default: The routing template maximizes system resources for unicast routing, typically required for a router in the center of a network.</td>
</tr>
<tr>
<td>dual-ipv4-and-ipv6</td>
<td>Supports both IPv4 and IPv6 routing.</td>
</tr>
<tr>
<td></td>
<td>This option is visible only when the switch supports IPv6 and IPv4 routing.</td>
</tr>
<tr>
<td></td>
<td>- default: Balance IPv4 and IPv6 Layer 2 and Layer 3 functionality.</td>
</tr>
</tbody>
</table>

**no sdm prefer**

Use this command to return to the default template.

<table>
<thead>
<tr>
<th>Format</th>
<th>no sdm prefer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Config</td>
</tr>
</tbody>
</table>

**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 used 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.

Use the optional keywords to list the scaling parameters of a specific template.

**Format**

```
show sdm prefer [dual-ipv4-and-ipv6 default | ipv4-routing {default | data-center} ]
```

**Mode**

Privileged EXEC

<table>
<thead>
<tr>
<th>Term</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>
<tr>
<td>IPv4 Multicast Routes</td>
<td>The maximum number of IPv4 multicast forwarding table entries.</td>
</tr>
<tr>
<td>IPv6 Multicast Routes</td>
<td>The maximum number of IPv6 multicast forwarding table entries.</td>
</tr>
</tbody>
</table>

Example:

```
#show sdm prefer
Current template: Dual IPv4 and IPv6
ARP Entries................................. 4096
IPv4 Unicast Routes....................... 6112
IPv6 NDP Entries........................... 2040
IPv6 Unicast Routes....................... 3072
ECMP Next Hops......................... 41
IPv4 Multicast Routes.................. 256
IPv6 Multicast Routes.................. 256
```

**IPv6 Management Commands**

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (that is, independent from the IPv6 Routing package). For Routing/IPv6 builds of Switch CLI dual IPv4/IPv6 operation over the service port is enabled. Switch CLI has capabilities such as:

- Static assignment of IPv6 addresses and gateways for the network ports.
- The ability to ping an IPv6 link-local address over the network port.
• Using IPv6 Management commands, you can send SNMP traps and queries via the network port.
• The user can manage a device via the network port (in addition to a routing interface).

**network ipv6 enable**

Use this command to enable IPv6 operation on the network port.

*Default* enabled

*Format* `network ipv6 enable`

*Mode* Privileged EXEC

**no network ipv6 enable**

Use this command to disable IPv6 operation on the network port.

*Format* `no network ipv6 enable`

*Mode* Privileged EXEC

**network ipv6 address**

Use this command to configure an IPv6 global address, enable or disable stateless global address autoconfiguration, and enable or disable dhcpv6 client protocol information for the network port. You can configure multiple IPv6 addresses on the network port.

*Format* `network ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}`

*Mode* Privileged EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</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>

**no network ipv6 address**

Use this command to:

• Remove the manually configured IPv6 global address on the network port interface (with the `address` option).
- Disable the stateless global address autoconfiguration on the network port (with the `autoconfig` option).
- Disable the dhcpv6 client protocol on the network port (with the `dhcp` option).

**Format**

```
no network ipv6 address \{address/prefix-length [eui64] | autoconfig | dhcp\}
```

**Mode**  
Privileged EXEC

**network ipv6 gateway**

Use this command to configure IPv6 gateway (default routers) information for the network port. The gateway address is in IPv6 global or link-local address format.

**Format**

```
network ipv6 gateway <gateway-address>
```

**Mode**  
Privileged EXEC

**no network ipv6 gateway**

Use this command to remove IPv6 gateways on the network port interface.

**Format**

```
no network ipv6 gateway
```

**Mode**  
Privileged EXEC

**show network ndp**

Use this command to display NDP cache information for the network port.

**Default**  
enabled

**Format**

```
show network ndp
```

**Mode**  
- Privileged EXEC
- User EXEC

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of the interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC Address used.</td>
</tr>
<tr>
<td>isRtr</td>
<td>Specifies the router flag.</td>
</tr>
<tr>
<td>Neighbor State</td>
<td>The state of the neighbor cache entry. Possible values are: Reachable, Delay.</td>
</tr>
<tr>
<td>Age Updated</td>
<td>The time in seconds that has elapsed since an entry was added to the cache.</td>
</tr>
</tbody>
</table>

The following shows sample CLI display output for the command:

```
(switch) #show network ndp
```

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Age</th>
</tr>
</thead>
</table>

Management Commands

661
show network ipv6 dhcp statistics

Use this command to display 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>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Advertisement Packets Received</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 Packets Discarded</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>
<tr>
<td>DHCPv6 Rebind Packets Transmitted</td>
<td>The number of DHCPv6 Rebind packets transmitted on the network interface.</td>
</tr>
<tr>
<td>DHCPv6 Release Packets Transmitted</td>
<td>The number of DHCPv6 Release packets transmitted on the network interface.</td>
</tr>
<tr>
<td>Total DHCPv6 Packets Transmitted</td>
<td>The total number of DHCPv6 packets transmitted on the network interface.</td>
</tr>
</tbody>
</table>

The following example shows CLI display output for the command:

```
(switch)#show network ipv6 dhcp statistics
DHCPv6 Client Statistics
----------------------------------------
DHCPv6 Advertisement Packets Received................. 0
```
ProSafe Managed Switch

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

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
This chapter lists common log messages, 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 NETGEAR, Inc. in determining the root cause of such a problem.

**Note:** This chapter does not contain a complete list of all syslog messages.

This chapter contains the following sections:

- Core
- Utilities
- Management
- Switching
- QoS
- Routing/IPv6 Routing
- Multicast
- Stacking
- Technologies
- O/S Support
### Core

#### Table 3. 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 7000 series application.</td>
</tr>
</tbody>
</table>

#### Table 4. 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 intfNum(x) unit x slot x port x</td>
<td>Interface creation out of order</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: Failed to find interface at unit x slot x port x for event(x)</td>
<td>There is no mapping between the USP and Interface number</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: L7_DETACH out of order for intfNum(x) 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 intfNum(x) 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>
<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 intfNum(x)</td>
<td>A component responded with a fail indication for an interface event</td>
</tr>
<tr>
<td>NIM</td>
<td>NIM: Timeout event(x), intfNum(x) remainingMask = “xxxx”</td>
<td>A component did not respond before the NIM timeout occurred</td>
</tr>
</tbody>
</table>
Table 5. 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 Switch CLI.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_FILENAME</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 &lt;file name&gt; version &lt;version num&gt;</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>
<tr>
<td>SYSTEM</td>
<td>File &lt;filename&gt;: same version (version num) but the sizes (&lt;version size&gt;-&gt;&lt;expected version size) differ</td>
<td>The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>Migrating config file &lt;filename&gt; from version &lt;version num&gt; to &lt;version num&gt;</td>
<td>The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>Building Defaults</td>
<td>Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>sysapiCfgFileGet failed size = &lt;expected size of file&gt; version = &lt;expected version&gt;</td>
<td>Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.</td>
</tr>
</tbody>
</table>
## Log Messages

### Utilities

Table 6. Trap Mgr Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Mgr</td>
<td>Link Up/Down: unit/slot/port</td>
<td>An interface changed link state.</td>
</tr>
</tbody>
</table>

Table 7. 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 8. 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 9. 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>
<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 10. 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</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 11. 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. xxxxxx:xx</td>
<td>Unsupported LLDP packet received.</td>
</tr>
</tbody>
</table>

### Table 12. 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>

### Management

### Table 13. 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 14. 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>ewaNetHTTPEnd: 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 15. 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%x</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 16. 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 17. 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 18. 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>
</tbody>
</table>
Table 18. SSHD Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<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 19. 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, ssltConnectionTask</td>
<td>Exceeded maximum allowed SSLT connections.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Error creating Secure server socket IPv6</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 = YYYY, errno = ZZZZ</td>
<td>Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.</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 loading private key for SSL connection.</td>
</tr>
<tr>
<td>SSLT</td>
<td>SSLT: Error setting cipher list (no valid ciphers)</td>
<td>Failed while setting cipher list.</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 20. 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 READ_ONLY.</td>
<td>Invalid access level specified for the user. The access level is set to READ_ONLY. XXXX indicates the username.</td>
</tr>
<tr>
<td>User_Manager</td>
<td>Could not migrate config file XXXX from version YYY to ZZZZ. Using defaults.</td>
<td>Failed to migrate the config file. XXXX is the config file name. YYY is the old version number and ZZZZ is the new version number.</td>
</tr>
</tbody>
</table>

### Switching

### Table 21. 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 protectedPort</td>
<td>This appears when protectedPortCfgRWLock 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 intIfNum 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 intIfNum 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 a 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 callback has come before the protected port component is ready.</td>
</tr>
</tbody>
</table>
### Table 22. IP Subnet VLANS Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsubnet 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>IPsubnet 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>IPsubnet 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>IPsubnet 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>IPsubnet vlans</td>
<td>vlanIpSubnetCnfgrFinPhase1Process: could not delete avl semaphore</td>
<td>This appears when a semaphore deletion of this component fails.</td>
</tr>
<tr>
<td>IPsubnet 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>IPsubnet vlans</td>
<td>vlanIpSubnetSubnetDeleteApply: Failed</td>
<td>This appears when a dtl fails to delete an entry from the table</td>
</tr>
<tr>
<td>IPsubnet 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>IPsubnet 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 23. 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>vlanMacCnfgrInitPhase1Process: 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>vlanMacCnfgrFinPhase1Process: 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>
</tbody>
</table>
### Table 23. 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>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 24. 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 &lt;authorized/unauthorized&gt;, intf xxx</td>
<td>DTL call failed setting authorization state of the port</td>
</tr>
<tr>
<td>802.1X</td>
<td>dot1xApplyConfigData: Unable to &lt;enable/disable&gt; 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 25. 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>
</tbody>
</table>

---

Log Messages

675
Table 25. 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>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 26. 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, GarplIssueCmd, 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 pre-configuration.</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</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 27. 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 28. 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 29. 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 pre-configuration.</td>
</tr>
</tbody>
</table>

### Table 30. 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 pre-configuration.</td>
</tr>
</tbody>
</table>

### Table 31. 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>
**Table 32. 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 pre-configuration.</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, dot1qVlanTaggedMemberSetModify: 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 it’s member set via management.</td>
</tr>
</tbody>
</table>

**Table 33. 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 34. 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 pre-configuration.</td>
</tr>
</tbody>
</table>
Table 35. 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>pbVlanCfngrInitPhase2Process: 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>pbVlanCfngrInitPhase2Process: 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>pbVlanCfngrInitPhase2Process: 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>

Table 36. 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 37. CoS Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS</td>
<td>cosCfngrInitPhase3Process: 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 38. 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: &quot;policy name, intIfNum 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>

Routing/IPv6 Routing

Table 39. 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>
<tr>
<td>DHCP relay</td>
<td>processDhcpPacket: invalid DHCP packet type: %u\n</td>
<td>The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent.</td>
</tr>
</tbody>
</table>

Table 40. 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 (&quot;RTO&quot;) 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>
</tbody>
</table>
Log Messages

Table 40. OSPFv2 Log Messages (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<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 41. OSPFv3 Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3</td>
<td>Best route client deregistration failed for OSPFv3 Redist</td>
<td>OSPFv3 registers with the IPv6 routing table manager (&quot;RTO6&quot;) 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>OSPFv3</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>OSPFv3</td>
<td>The number of LSAs, 16992, in the OSPF LSDB has 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>
</tbody>
</table>
| OSPFv3    | LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted. | OSPFv3 periodically verifies the checksum of each LSA in memory. OSPFv3 logs this
### Table 42. Routing Table Manager Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table Manager</td>
<td>RTO is full. Routing table contains 8000 best routes, 8000 total routes.</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>
<tr>
<td>Routing Table Manager</td>
<td>RTO no longer full. Bad adds: 10. Routing table contains 7999 best routes, 7999 total 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>
</tbody>
</table>

### Table 43. VRRP Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP</td>
<td>Changing priority to 255 for virtual router with VRID 1 on interface 1/0/1</td>
<td>When the router is configured with the address being used as the virtual router ID, the router’s priority is automatically set to the maximum value to ensure that the address owner becomes the VRRP master.</td>
</tr>
<tr>
<td>VRRP</td>
<td>Changing priority to 100 for virtual router with VRID 1 on interface 1/0/1</td>
<td>When the router is no longer the address owner, Switch CLI reverts the router’s priority to the default.</td>
</tr>
<tr>
<td>VRRP</td>
<td>vrrpPacketValidate: Invalid TTL</td>
<td>VRRP ignored an incoming message whose time to live (TTL) in the IP header was not 255.</td>
</tr>
</tbody>
</table>

### Table 44. ARP Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>ARP received mapping for IP address xxx to MAC address yyy. This IP address may be configured on two stations.</td>
<td>When we receive an ARP response with different MAC address from another station with the same IP address as ours. This might be a case of misconfiguration.</td>
</tr>
</tbody>
</table>
Table 45. 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>

Table 46. DHCP6 Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP6</td>
<td>relay_to_server: Cannot relay to relay server intf xxx: not IPv6 enabled</td>
<td>Relay is enabled but neither the outgoing interface nor the server IP address is specified.</td>
</tr>
</tbody>
</table>

Multicast

Table 47. Cache Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache</td>
<td>Out of memory when creating entry.</td>
<td>When we run out of memory while creating a new cache (MFC) entry</td>
</tr>
<tr>
<td>Cache</td>
<td>Out of memory when creating cache.</td>
<td>When we run out of memory while creating the cache itself</td>
</tr>
</tbody>
</table>

Table 48. IGMP Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP</td>
<td>Error creating IGMP pipe</td>
<td>When we fail to create / open IGMP pipe for Mcast control messages</td>
</tr>
<tr>
<td>IGMP</td>
<td>Error opening IGMP pipe</td>
<td>When we fail to create / open IGMP data pipe for Mcast data messages</td>
</tr>
<tr>
<td>IGMP</td>
<td>Error getting memory for source record</td>
<td>When we are unable to allocate memory for a source record in the received IGMP V3 report</td>
</tr>
<tr>
<td>IGMP</td>
<td>Failed getting memory for new group</td>
<td>When we are unable to allocate memory for a group record in the received IGMP V3/V2/V1 report</td>
</tr>
</tbody>
</table>
Table 49. IGMP-Proxy Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP-Proxy</td>
<td>Error getting memory for igmp host group record</td>
<td>When we are unable to allocate memory for the IGMP group record in the Host (Proxy) table</td>
</tr>
<tr>
<td>IGMP-Proxy</td>
<td>Error getting memory for source record</td>
<td>When we are unable to allocate memory for the IGMP source record in the Host (Proxy) table</td>
</tr>
</tbody>
</table>

Table 50. PIM-SM Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM-SM</td>
<td>PIM-SM not initialized</td>
<td>This message arises when trying to activate pimsm interfaces or receiving pimsm packets when pimsm component is not initialized.</td>
</tr>
<tr>
<td>PIM-SM</td>
<td>Unable to take xxx semaphore</td>
<td>This message is logged when failed to acquire semaphore to access source list or group list or candidate Rp list or virtual interface list. The xxx specifies the list for which the access is denied.</td>
</tr>
<tr>
<td>PIM-SM</td>
<td>Warning : Could not send packet type xxx (pimsm packet type) on rtrIfNum</td>
<td>This warning is logged when failed to send a pimsm control packet on the specified router interface.</td>
</tr>
<tr>
<td>PIM-SM</td>
<td>add_kernel_cache : memory allocation failed</td>
<td>This message is logged when there is insufficient memory to add an mroute entry into cache.</td>
</tr>
<tr>
<td>PIM_SMI</td>
<td>Config error. Trying to add static RP. Dynamic RP with same ip addr exists</td>
<td>Router learns RP-group mapping through Bootstrap messages received. This message pops when the static RP is configured which conflicts the mapping learnt dynamically through Bootstrap messages.</td>
</tr>
<tr>
<td>PIM-SM</td>
<td>Inner xxx(source/group) address of register message is invalid</td>
<td>This log message appears when a register message is received with invalid inner ip source or group address.</td>
</tr>
</tbody>
</table>
Table 51. PIM-DM Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM-DM</td>
<td>Out of memory when creating xxx</td>
<td>This message is logged when there is insufficient memory to accommodate a new neighbor/(S,G) Entry, Prune, Graft, Join etc.</td>
</tr>
<tr>
<td>PIM-DM</td>
<td>Error entry-&gt;ll_xxx LL creation error</td>
<td>This message is logged when the SLL creation is Failed.</td>
</tr>
<tr>
<td>PIM-DM</td>
<td>pim Interface_set: Could not give taskSema</td>
<td>This message is logged when Task synchronization Semaphore release fails.</td>
</tr>
<tr>
<td>PIM-DM</td>
<td>Error initializing CACHE</td>
<td>This message is logged when the PIM-DM (S,G) entry Cache table initialization fails.</td>
</tr>
<tr>
<td>PIM-DM</td>
<td>Error creating PIM-DM pipe</td>
<td>This message is logged when the PIM-DM Pipe (that receives control messages) creation fails.</td>
</tr>
</tbody>
</table>

Table 52. DVMRP Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVMRP</td>
<td>dvmrp_send_graft: failed getting memory for graft</td>
<td>Failed to allocate memory while sending a graft</td>
</tr>
<tr>
<td>DVMRP</td>
<td>dvmrp_register_neighbor: failed getting memory for nbr</td>
<td>Failed to allocate memory while registering a neighbor</td>
</tr>
<tr>
<td>DVMRP</td>
<td>dvmrp_recv_prune: failed getting memory for prune</td>
<td>Failed to allocate memory while receiving a prune</td>
</tr>
<tr>
<td>DVMRP</td>
<td>dvmrp_new_route: failed getting memory for route</td>
<td>Failed to get memory for a new route entry</td>
</tr>
<tr>
<td>DVMRP</td>
<td>dvmrp_prepare_routes: failed getting memory for dvmrp_ann_rt</td>
<td>Failed to get memory while announcing a new route entry</td>
</tr>
</tbody>
</table>

Stacking

Table 53. EDB Log Message

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDB</td>
<td>EDB Callback: Unit Join: &lt;num&gt;.</td>
<td>Unit &lt;num&gt; has joined the stack.</td>
</tr>
<tr>
<td>Component</td>
<td>Message</td>
<td>Cause</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OS</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>OS</td>
<td>In hapiBroadSystemMacAddress call to 'bcm_i2_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>OS</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>OS</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>OS</td>
<td>ERROR: policy x, tmpPolicy x, size x, data 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>OS</td>
<td>ACL x not found in internal table</td>
<td>Attempting to delete a non-existent ACL</td>
</tr>
<tr>
<td>OS</td>
<td>ACL internal table overflow</td>
<td>Attempting to add an ACL to a full table</td>
</tr>
<tr>
<td>OS</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>OS</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>OS</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>OS</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>OS</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>OS</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>OS</td>
<td>USL: A Trunk doesn’t exist in USL</td>
<td>Attempting to modify a Trunk that doesn’t exist</td>
</tr>
</tbody>
</table>
### Table 54. System General Error Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</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>OS</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>OS</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>OS</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>OS</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>OS</td>
<td>USL: Mcast entry not found on a leave</td>
<td>Possible synchronization issue between the application, hardware, and sync layer</td>
</tr>
<tr>
<td>OS</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>OS</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>OS</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>OS</td>
<td>Invalid LAG id x</td>
<td>Possible synchronization issue between the BCM driver and HAPI</td>
</tr>
<tr>
<td>OS</td>
<td>Invalid uport calculated from the BCM uport bcmx_l2_addr-&gt;lport = x</td>
<td>Uport not valid from BCM driver.</td>
</tr>
<tr>
<td>OS</td>
<td>Invalid USP calculated from the BCM uportinbcmx_l2_addr-&gt;lport = x</td>
<td>USP not able to be calculated from the learn event for BCM driver.</td>
</tr>
<tr>
<td>OS</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>OS</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>OS</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>OS</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>
</tbody>
</table>
Table 54. System General Error Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</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>OS</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>OS</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>OS</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>

Table 55. OSAPI Log Messages

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSAPI</td>
<td>ftruncate failed – File resides on a read-only file system.</td>
<td>ftruncate is called to correctly set the file’s size in the file system after a write. The file system is R/W so this msg indicates the file system may be corrupted.</td>
</tr>
<tr>
<td>OSAPI</td>
<td>ftruncate failed – File is open for reading only.</td>
<td>ftruncate is called to correctly set the file’s size in the file system after a write. The file is opened for R/W so this msg indicates the file system may be corrupted.</td>
</tr>
<tr>
<td>OSAPI</td>
<td>ftruncate failed – File descriptor refers to a file on which this operation is impossible.</td>
<td>ftruncate is called to correctly set the file’s size in the file system after a write. This msg indicates the file system may be corrupted.</td>
</tr>
<tr>
<td>OSAPI</td>
<td>ftruncate failed – Returned an unknown code in errno.</td>
<td>ftruncate is called to correctly set the file’s size in the file system after a write. This msg indicates the file system may be corrupted.</td>
</tr>
<tr>
<td>OSAPI</td>
<td>ping: bad host!</td>
<td>The address requested to ping can not be converted to an Internet address.</td>
</tr>
<tr>
<td>OSAPI</td>
<td>osapiTaskDelete: Failed for (XX) error YYY</td>
<td>The requested task can not be deleted because: the requested deletion is called from an ISR, the task is already deleted, or the task ID is invalid.</td>
</tr>
</tbody>
</table>
Table 55. OSAPI Log Messages (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSAPI</td>
<td>osapiCleanupIf: NetIPGet</td>
<td>During the call to remove the interface from the route table, the attempt to get an ipv4 interface address from the stack failed.</td>
</tr>
<tr>
<td>OSAPI</td>
<td>osapiCleanupIf: NetMaskGet</td>
<td>During the call to remove the interface from the route table, the attempt to get the ipv4 interface mask from the stack failed.</td>
</tr>
<tr>
<td>OSAPI</td>
<td>osapiCleanupIf: NetIpDel</td>
<td>During the call to remove the interface from the route table, the attempt to delete the primary ipv4 address from the stack failed.</td>
</tr>
<tr>
<td>OSAPI</td>
<td>osapiSemaTake failed</td>
<td>The requested semaphore can not be taken because: the call is made from an ISR or the semaphore ID is invalid.</td>
</tr>
</tbody>
</table>
The Captive Portal feature is a software implementation that blocks clients from accessing the network until user verification has been established. Verification can be configured to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted.

The Authentication server supports both HTTP and HTTPS web connections. In addition, Captive Portal can be configured to use an optional HTTP port (in support of HTTP Proxy networks). If configured, this additional port is then used exclusively by Captive Portal. Note that this optional port is in addition to the standard HTTP port 80 which is currently being used for all other web traffic.

This chapter contains the following sections:

- Captive Portal Global Commands
- Captive Portal Configuration Commands
- Captive Portal Status Commands
- Captive Portal Client Connection Commands
- Captive Portal Interface Commands
- Captive Portal Local User Commands
- Captive Portal User Group Commands

## Captive Portal Global Commands

The commands in this section are related to Captive Portal Global configurations.

```plaintext
captive-portal
```

Use this command to enter the captive portal configuration mode.

<table>
<thead>
<tr>
<th>Format</th>
<th>captive-portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Global Configuration mode</td>
</tr>
</tbody>
</table>
enable

Use this command to globally enable captive portal.

Default: disabled
Format: enable
Mode: Captive Portal Configuration mode

no enable

Use this command to globally disable captive portal.

Default: disabled
Format: no enable
Mode: Captive Portal Configuration mode

http port

Use this command to configure an additional HTTP port for captive portal to monitor. The valid range is from 0 to 65535.

Default: 80
Format: http port <0-65535>
Mode: Captive Portal Configuration mode

no http port

Use this command to reset the HTTP port to the default number 80.

Format: no http port
Mode: Captive Portal Configuration mode

https port

Use this command to configure an additional HTTPS port for captive portal to monitor. The valid range is from 0 to 65535.

Default: 443
Format: https port <0-65535>
Mode: Captive Portal Configuration mode
no https port

Use this command to reset the HTTPs port to the default HTTPS port 443.

Format: `no https port`
Mode: Captive Portal Configuration mode

authentication timeout

Use this command to configure the authentication timeout. If the user does not enter valid credentials within this time limit, the authentication page needs to be served again in order for the client to gain access to the network.

Default: 300
Format: `authentication timeout <60-600>`
Mode: Captive Portal Configuration mode

no authentication timeout

Use this command to reset the authentication timeout to the default.

Default: 300
Format: `no authentication timeout`
Mode: Captive Portal Configuration mode

show captive-portal

Use this command to display the status of the captive portal feature.

Format: `show captive-portal`
Mode: Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Mode</td>
<td>The administrative mode is enabled or disabled.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The Operational status is enabled or disabled.</td>
</tr>
<tr>
<td>Disable Reason</td>
<td>If the operational status is disabled. This field shows the reason why the operational is disabled.</td>
</tr>
<tr>
<td>CP IP Address</td>
<td>It is the captive portal server IP address.</td>
</tr>
</tbody>
</table>

Example

```
(switch)#show captive-portal
```
ProSafe Managed Switch

Administrative Mode....................... Disabled
Operational Status....................... Disabled
Disable Reason......................... Administrator Disabled
CP IP Address................. 1.2.3.4

**show captive-portal status**

Use this command to report the status of all captive portal instances in the system.

**Format**

```
show captive-portal status
```

**Mode**

Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional HTTP Port</td>
<td>The additional HTTP port for captive portal to monitor. Captive portal only monitors port 80 by default.</td>
</tr>
<tr>
<td>Additional HTTP Secure Port</td>
<td>The additional HTTPs port for captive portal to monitor. Captive portal only monitors port 443 by default.</td>
</tr>
<tr>
<td>Peer Switch Statistics Reporting Interval</td>
<td>The timeout for the authentication page to be served again.</td>
</tr>
<tr>
<td>Supported Captive Portals</td>
<td>The maximum number of captive portal instances supported by switch. It supports up to 10 instances.</td>
</tr>
<tr>
<td>Configured Captive Portals</td>
<td>The number of created captive portal instances.</td>
</tr>
<tr>
<td>Active Captive Portals</td>
<td>The number of active captive portal instances.</td>
</tr>
<tr>
<td>System Supported Users</td>
<td>The maximum number of user can be authenticated.</td>
</tr>
<tr>
<td>Local Supported Users</td>
<td>The maximum number of local user can be created.</td>
</tr>
<tr>
<td>Authenticated Users</td>
<td>The number of the authenticated users.</td>
</tr>
</tbody>
</table>

**Example**

```
(switch)#show captive-portal status
Additional HTTP Port......................... 0
Additional HTTP Secure Port............... 0
Peer Switch Statistics Reporting Interval.... 120
Authentication Timeout......................... 300
Supported Captive Portals................. 10
Configured Captive Portals............... 1
Active Captive Portals.................... 0
System Supported Users.................... 1024
Local Supported Users.................... 128
Authenticated Users.................... 0
```
Captive Portal Configuration Commands

The commands in this section are related to captive portal configurations.

**configuration (Captive Portal)**

Use this command to enter the captive portal instance mode. The captive portal configuration identified by CP ID 1 is the default CP configuration. The system supports a total of ten CP configurations.

<table>
<thead>
<tr>
<th>Format</th>
<th>configuration &lt;1-10&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Captive Portal Configuration mode</td>
</tr>
</tbody>
</table>

**no configuration**

Use this command to delete a CP configuration. The default configuration cannot be deleted.

<table>
<thead>
<tr>
<th>Format</th>
<th>no configuration &lt;1-10&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Captive Portal Configuration mode</td>
</tr>
</tbody>
</table>

**enable (Instance)**

Use this command to enable a captive portal configuration.

<table>
<thead>
<tr>
<th>Default</th>
<th>enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>enable</td>
</tr>
<tr>
<td>Mode</td>
<td>Captive Portal Instance mode</td>
</tr>
</tbody>
</table>

**no enable**

Use this command to disable a configuration.

<table>
<thead>
<tr>
<th>Default</th>
<th>enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>no enable</td>
</tr>
<tr>
<td>Mode</td>
<td>Captive Portal Instance mode</td>
</tr>
</tbody>
</table>

**name**

Use this command to configure the name for a captive portal configuration. The cp-name can be up to 32 alphanumeric characters in length.

| Default      | Configuration 1 has the name “Default” by default. All other configurations have no name by default. |
### Captive Portal Commands

<table>
<thead>
<tr>
<th>Format</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>no name</td>
<td>Captive Portal Instance mode</td>
</tr>
<tr>
<td>protocol</td>
<td>Captive Portal Instance mode</td>
</tr>
<tr>
<td>verification</td>
<td>Captive Portal Instance mode</td>
</tr>
<tr>
<td>group</td>
<td>Captive Portal Instance mode</td>
</tr>
</tbody>
</table>

**no name**

Use this command to remove a configuration name.

**Format**

```plaintext```
no name
```

**Mode**

Captive Portal Instance mode

**protocol**

Use this command to configure the protocol mode for a captive portal configuration. The default protocol is http.

**Default**

```plaintext```
http
```

**Format**

```plaintext```
protocol { http | https }
```

**Mode**

Captive Portal Instance mode

**verification**

Use this command to configure the verification mode for a captive portal configuration. User verification can be configured to allow access for guest users; users that do not have assigned user names and passwords. User verification can also be configured to allow access for authenticated users. Authenticated users are required to enter a valid user name and password that must first be validated against the local database or a RADIUS server. Network access is granted once user verification has been confirmed.

**Default**

```plaintext```
guest
```

**Format**

```plaintext```
verification { guest | local | radius }
```

**Mode**

Captive Portal Instance mode

**group**

Use this command to configure a group ID for this captive portal configuration. If a group number is configured, the user entry (Local or RADIUS) must be configured with the same name and the group to authenticate to this captive portal instance. The group ID must be assigned first. If it isn’t, use the `user group <1-10>` command to create the group ID. The default group ID is 1 for a captive portal configuration.

**Default**

```plaintext```
1
```

**Format**

```plaintext```
group <1-10>
```

**Mode**

Captive Portal Instance mode
no group

Use this command to reset the group number to the default.

Default  1
Format    no group <1-10>
Mode     Captive Portal Instance mode

redirect (Captive Portal)

Use this command to enable the redirect mode for a captive portal configuration. Use the “no” form of this command to disable redirect mode.

Default  disable
Format    redirect
Mode     Captive Portal Instance mode

no redirect

Use this command to disable redirect mode.

Format    no redirect
Mode     Captive Portal Instance mode

redirect-url

Use this command to configure the redirect URL for a captive portal configuration. The url is the URL for redirection which can be up to 512 characters in length.

Format    redirect-url url
Mode     Captive Portal Instance mode

max-bandwidth-down

Use this command configures the maximum rate at which a client can receive data from the network. The rate is in bits per seconds. 0 indicates limit not enforced.

Default  0
Format    max-bandwidth-down <0-536870911>
Mode     Captive Portal Instance mode
no max-bandwidth-down

Use this command to reset the maximum rate to the default.

**Format**

```
no max-bandwidth-down
```

**Mode**

Captive Portal Instance mode

max-bandwidth-up

Use this command to configure the maximum rate at which a client can send data into the network. The rate is in bits per seconds. 0 indicates limit not enforced.

**Default**

0

**Format**

```
max-bandwidth-up <0-536870911>
```

**Mode**

Captive Portal Instance mode

no max-bandwidth-up

Use this command to reset the maximum rate to the default.

**Format**

```
no max-bandwidth-up
```

**Mode**

Captive Portal Instance mode

max-input-octets

Use this command to configure the maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. The number of octets is in bytes. 0 indicates limit not enforced.

**Default**

0

**Format**

```
max-input-octets <0-4294967295>
```

**Mode**

Captive Portal Instance mode

no max-input-octets

Use this command to reset the limit to the default.

**Format**

```
no max-input-octets
```

**Mode**

Captive Portal Instance mode
**max-output-octets**

Use this command to configure the maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. The number of octets is in bytes. 0 indicates limit not enforced. Use the “no”.

**Default**

0

**Format**

max-output-octets <0-4294967295>

**Mode**

Captive Portal Instance mode

**no max-output-octets**

Use this command to reset the limit to the default.

**Format**

no max-output-octets

**Mode**

Captive Portal Instance mode

**max-total-octets**

Use this command to configure the maximum number of octets the user is allowed to transfer; that is, the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. The number of total octets is in bytes. 0 indicates limit not enforced. Use the “no” form of this command to reset the limit to the default.

**Default**

0

**Format**

max-total-octets <0-4294967295>

**Mode**

Captive Portal Instance mode

**no max-total-octets**

Use this command to reset the limit to the default.

**Default**

0

**Format**

max-total-octets <0-4294967295>

**Mode**

Captive Portal Instance mode

**session-timeout (Captive Portal)**

Use this command to configure the session timeout for a captive portal configuration. After this limit has been reached, the user will be disconnected. Timeout is time in seconds. 0 indicates timeout not enforced.

**Default**

0

**Format**

session-timeout <0-86400>

**Mode**

Captive Portal Instance mode
no session-timeout

Use this command to reset the session timeout to the default.

Format       session-timeout <0-86400>
Mode         Captive Portal Instance mode

idle-timeout

Use this command to configure the idle timeout for a captive portal configuration. 0 indicates timeout not enforced. After an idle session has been reached this, the user will be disconnected.

Default      0
Format        idle-timeout <0-900>
Mode          Captive Portal Instance mode

no idle-timeout

Use this command to reset the idle timeout to the default.

Format       no idle-timeout
Mode          Captive Portal Instance mode

locale

This command is not intended to be a user command. The administrator must use the WEB UI to create and customize captive portal web content. This command is primarily used by the show running-config command and process as it provides the ability to save and restore configurations using a text based format.

Default      1
Format        locale <1-5>
Mode          Captive Portal Instance mode

no locale

This command is intended to delete a locale. The default locale cannot be deleted.

Format       no locale <1-5>
Mode          Captive Portal Instance mode
**interface (Captive Portal)**

Use this command to associate an interface with a captive portal configuration.

**Format**
```
interface <unit/slot/port>
```

**Mode**
Captive Portal Instance Config mode

**no interface**

Use this command to remove an association with a captive portal configuration.

**Format**
```
no interface <unit/slot/port>
```

**Mode**
Captive Portal Instance Config mode

**block**

Use this command to block all traffic for a captive portal configuration. The administrator can block access to a captive portal configuration. When an instance is blocked no client traffic is allowed through any interfaces associated with that captive portal configuration. Blocking a captive portal instance is a temporary command executed by the administrator and not saved in the configuration.

**Default**
```
no block
```

**Format**
```
block
```

**Mode**
Captive Portal Instance mode

**no block**

Use this command to unblock traffic.

**Format**
```
no block
```

**Mode**
Captive Portal Instance mode

**Captive Portal Status Commands**

This section describes commands that return captive portal status.

**show captive-portal configuration**

Use this command to display the operational status of each captive portal configuration.

**Format**
```
show captive-portal configuration <1-10>
```

**Mode**
Privileged EXEC mode
Captive Portal Commands

ProSafe Managed Switch

Example

(switch)#show captive-portal configuration 1
CP ID................................. 1
CP Name............................... cp1
Operational Status.................. Disabled
Disable Reason...................... Administrator Disabled
Blocked Status...................... Not Blocked
Authenticated Users................. 0

show captive-portal configuration interface

Use this command to display information about all interfaces assigned to a captive portal configuration or about a specific interface assigned to a captive portal configuration. The <1-10> is the captive portal ID. If you do not specify an interface number, all the interfaces assigned to the captive portal configuration will be displayed.

Format

show captive-portal configuration <1-10> interface [ <unit/slot/port> ]

Mode

Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP ID</td>
<td>The captive portal ID</td>
</tr>
<tr>
<td>CP Name</td>
<td>The captive portal instance name</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface associated with the CP ID</td>
</tr>
<tr>
<td>Interface Description</td>
<td>The interface description</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The operational status is enabled or disabled.</td>
</tr>
<tr>
<td>Disable Reason</td>
<td>The reason if the operational status is disabled.</td>
</tr>
<tr>
<td>Block Status</td>
<td>It shows this captive portal instance block all traffic or not.</td>
</tr>
</tbody>
</table>
If the interface is specified. The following term will be displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated users</td>
<td>The number of authenticated users associated with the CP ID.</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
(Switch)#show captive-portal configuration 1 interface
CP ID................................. 1
CP Name................................. cp1
Interface................................. 1/0/1
Interface Description..................... Unit: 1 Slot: 0 Port: 1 Gigabit
Operational Status......................... Disabled
Disable Reason............................ Interface Not Attached
Block Status................................ Not Blocked
Authenticated Users........................ 0

(Switch)#show captive-portal configuration 1 interface 1/0/1
CP ID................................. 1
CP Name................................. cp1
Interface................................. 1/0/1
Interface Description..................... Unit: 1 Slot: 0 Port: 1 Gigabit
Operational Status......................... Disabled
Disable Reason........................... Interface Not Attached
Block Status............................. Not Blocked
Authenticated Users....................... 0
```

**show captive-portal configuration status**

Use this command to display information about all configured captive portal configurations or about a specific captive portal configuration. The `<1-10>` is captive portal ID. If `<1-10>` is not entered, all the configurations are displayed.

**Format**

```plaintext
show captive-portal configuration [ <1-10> ] status
```

**Mode**

Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP ID</td>
<td>The captive portal instance ID</td>
</tr>
<tr>
<td>CP Name</td>
<td>The captive portal instance name</td>
</tr>
<tr>
<td>Mode</td>
<td>The operational mode is enabled or disabled.</td>
</tr>
<tr>
<td>Protocol Mode</td>
<td>The protocol mode is https or http.</td>
</tr>
<tr>
<td>Verification Mode</td>
<td>The user verification mode has three modes: guest, local and radius. The default is guest mode.</td>
</tr>
</tbody>
</table>
If the interface is specified, the following terms are displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the group associated with this captive portal instance.</td>
</tr>
<tr>
<td>Redirect URL Mode</td>
<td>The redirect mode for this captive portal instance.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>The redirect URL is up to 512 characters.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Logout once session timeout is reached (seconds).</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Logout once idle timeout is reached (seconds).</td>
</tr>
<tr>
<td>Max Bandwidth Up</td>
<td>Maximum client transmit rate (b/s). Limits the bandwidth at which the client can send data into the network.</td>
</tr>
<tr>
<td>Max Bandwidth Down</td>
<td>Maximum client receive rate (b/s). Limits the bandwidth at which the client can receive data from the network.</td>
</tr>
<tr>
<td>Max Input Octets</td>
<td>Maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected.</td>
</tr>
<tr>
<td>Max Output Octets</td>
<td>Maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected.</td>
</tr>
<tr>
<td>Max Total Octets</td>
<td>Maximum number of octets the user is allowed to transfer (sum of octets transmitted and received). After this limit has been reached the user will be disconnected.</td>
</tr>
</tbody>
</table>

Example

```
(switch)#show captive-portal configuration status
CP ID     CP Name        Mode     Protocol    Verification
-----    ----------    --------   --------    ------------
1          cp1          Enable     https       Guest
2          cp2          Enable     http        Local
3          cp3          Disable    https       Guest
(switch)#show captive-portal configuration 1 status
CP ID.......................................... 1
CP Name........................................ cp1
Mode........................................... Enabled
Protocol Mode.................................. https
Verification Mode.............................. Guest
Group Name..................................... group123
Redirect URL Mode.............................. Enabled
Redirect URL................................... www.cnn.com
Session Timeout (seconds)...................... 86400
Idle Timeout (seconds)......................... 600
Max Bandwidth Up (bytes/sec)............... 0
Max Bandwidth Down (bytes/sec)............. 0
Max Input Octets (bytes)..................... 0
Max Output Octets (bytes)................... 0
Max Total Octets (bytes).................... 0
```
**show captive-portal configuration locales**

Use this command to display locales associated with a specific captive portal configuration. `<1-10>` is captive port ID.

Format: `show captive-portal configuration <1-10> locales`

Mode: Privileged EXEC mode

**Example**

```
(switch)#show captive-portal configuration 1 locales
Locale Code
---------------
En
```

**show captive-portal trapflags**

Use this command to display which captive portal traps are enabled.

Format: `show captive-portal trapflags`

Mode: Privileged EXEC mode

**Example**

```
(switch)#show captive-portal trapflags
Client Authentication Failure Traps............ Disable
Client Connection Traps........................ Disable
Client Database Full Traps..................... Disable
Client Disconnection Traps..................... Disable
```

**Captive Portal Client Connection Commands**

This section describes captive portal client connection commands.

**show captive-portal client status**

Use this command to display client connection details or a connection summary for connected captive portal users. `macaddr` is Client MAC address. If no `macaddr` is entered, all the client status will be displayed.

Format: `show captive-portal client [ macaddr ] status`

Mode: Privileged EXEC mode
### Term | Definition
--- | ---
Client MAC Address | The MAC address of the authenticated user
Client IP Address | The IP address of the authenticated user
Protocol | The protocol the user is using to access the network.
Verification | The verification mode for this client.
Session Time | The current session time since the client is authenticated.

If the macaddr is specified, the following terms are displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP ID</td>
<td>The captive portal ID associated with the client</td>
</tr>
<tr>
<td>CP Name</td>
<td>The captive portal name associated with the client</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface on which the client authenticated.</td>
</tr>
<tr>
<td>Interface Description</td>
<td>The interface description</td>
</tr>
<tr>
<td>User Name</td>
<td>The name of the client who is authenticated.</td>
</tr>
</tbody>
</table>

#### Example

```
(switch)#show captive-portal client status
Client MAC Address  Client IP Address  Protocol  Verification  Session Time
-----------------   ----------------   --------  ------------   -----  
0002.BC00.1290    10.254.96.47       https     Local     0d:00:00:13
0002.BC00.1291    10.254.96.48       https     Local     0d:00:05:20
0002.BC00.1292    10.254.96.49       https     Radius    0d:00:00:20

(switch)#show captive-portal client 0002.BC00.1290 status
Client MAC Address........................ 0002.BC00.1290
Client IP Address......................... 10.254.96.47
Protocol Mode................................ https
Verification Mode.......................... Local
CP ID...................................... 1
CP Name.................................... cp1
Interface.................................. 1/0/1
Interface Description...................... Unit: 1 Slot: 0 Port: 1 Gigabit - Level
User Name.................................. user123
Session Time.............................. 0d:00:00:13
```
show captive-portal client statistics

Use this command to display the statistics for a specific captive portal client. The macaddr is client MAC address.

**Format**

`show captive-portal client <macaddr> statistics`

**Mode**

Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client MAC address</td>
<td>The MAC address of the authenticated client</td>
</tr>
<tr>
<td>Bytes Received</td>
<td>The number of bytes received from the client</td>
</tr>
<tr>
<td>Bytes Transmitted</td>
<td>The number of bytes transmitted to the client</td>
</tr>
<tr>
<td>Packets Received</td>
<td>The number of packets received from the client</td>
</tr>
<tr>
<td>Packets Transmitted</td>
<td>The number of packets transmitted from the client</td>
</tr>
</tbody>
</table>

**Example**

```
(switch)#show captive-portal client 0102.0304.0506 statistics
Client MAC Address......................... 0002.bc00.1290
Bytes Received............................ 0
Bytes Transmitted......................... 0
Packets Received.......................... 0
Packets Transmitted....................... 0
```

show captive-portal interface client status

Use this command to display information about clients authenticated on all interfaces or a specific interface.

**Format**

`show captive-portal interface [<unit/slot/port>] client status`

**Mode**

Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Intf</td>
<td>Interface on which the clients are authenticated.</td>
</tr>
<tr>
<td>Client Intf Description</td>
<td>The interface description</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the authenticated user.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the authenticated user.</td>
</tr>
</tbody>
</table>
If the interface is specified, the following terms are displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP ID</td>
<td>The ID of the captive portal associated with the client</td>
</tr>
<tr>
<td>CP Name</td>
<td>The name of the captive portal associated with the client</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol the client is using</td>
</tr>
<tr>
<td>Verification</td>
<td>The user verification mode</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
(switch)#show captive-portal interface client status
Client          Client
Intf     Intf Description                          MAC Address          IP Address
------  -------------------------------     -----------------  ---------------
1/0/1   Unit: 1 Slot: 0 Port: 1 Gigabit     0002.BC00.1290      10.254.96.47
1/0/2   Unit: 1 Slot: 0 Port: 2 Gigabit     0002.BC00.1292      10.254.96.49
1/0/3   Unit: 1 Slot: 0 Port: 3 Gigabit     0002.BC00.1293      10.254.96.50
```

```plaintext
(switch)#show captive-portal interface 1/0/1 client status
Interface......................... 1/0/1
Interface Description............... Unit: 1 Slot: 0 Port: 1 Gigabit
Client Client
MAC Address         IP Address     CP ID     CP Name     Protocol     Verification
-----------------         ---------------    -----      --------------    --------     ------------
0002.BC00.1290    10.254.96.47   1              cp1               http            local
0002.BC00.1291    10.254.96.48   2              cp2               http            local
```

**show captive-portal configuration client status**

Use this command to display the clients authenticated to all captive portal configurations or a specific configuration. `<1-10>` is the captive portal ID.

**Format**

```
show captive-portal configuration [ <1-10> ] client status
```

**Mode**

Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP ID</td>
<td>The captive portal ID</td>
</tr>
<tr>
<td>CP Name</td>
<td>The captive portal name</td>
</tr>
<tr>
<td>Client MAC Address</td>
<td>The MAC address of the client associated with the captive portal instance.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>The IP address of the client associated with the captive portal instance.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface on which the client is authenticated.</td>
</tr>
</tbody>
</table>
If the CP ID is specified, the following terms are displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The description of the interface</td>
</tr>
</tbody>
</table>

Example

```
(switch)#show captive-portal configuration client status
CP ID  CP Name  Client MAC Address    Client IP Address   Interface
-----  -------  ------------------    -----------------  ---------
1      cp1     0002.BC00.1290       10.254.96.47        1/0/1
2      cp2     0002.BC00.1292       10.254.96.49        1/0/3
3      cp3     0002.BC00.1293       10.254.96.50        1/0/4
```

```
(switch)#show captive-portal configuration 1 client status
CP ID..................................... 1
CP Name................................... cp1
Client            Client
MAC Address      IP Address     Interface    Interface Description
--------------   -------------  ---------    ----------------------
0002.BC00.1290   10.254.96.47    1/0/1   Unit:1 Slot:0 Port:1 Gigabit
0002.BC00.1291   10.254.96.48    1/0/2   Unit:1 Slot:0 Port:2 Gigabit
```

captive-portal client deauthenticate

Use this command to deauthenticate a specific captive portal client. The `macaddr` is the Client MAC address.

Format: captive-portal client deauthenticate [macaddr]|<1-10>

Mode: Privileged EXEC mode

Captive Portal Interface Commands

The following section describes captive portal interface commands.

show captive-portal interface configuration status

Use this command to display the interface to configuration assignments for all captive portal configurations or for a specific configuration. `<1-10>` is the captive portal ID.

Format: show captive-portal interface configuration [ <1-10> ] status

Mode: Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP ID</td>
<td>The captive portal ID</td>
</tr>
<tr>
<td>CP Name</td>
<td>The captive portal name</td>
</tr>
</tbody>
</table>
### Captive Portal Commands

#### Captive Portal Local User Commands

The following section describes captive portal local user commands.

**user password**

Use this command to create a local user or change the password for an existing user. The *user-id* is user ID in the range of 1-128. The *password* is the user password in the range of 8-64 characters. You can also enter encrypted password using the parameter *encrypted*.

**Format**

```plaintext
user user-id password { password | encrypted enc-password }
```

**Mode**

Captive Portal Configuration mode

**no user**

Use this command to delete a user from the local user database. If the user has an existing session, it is disconnected.

**Format**

```plaintext
no user user-id <1-128>
```

**Mode**

Captive Portal Configuration mode
**user name**

Use this command to modify the user name for a local captive portal user. `<1-128>` is the user ID and the name is the user name in the range of 1-32 characters. The local user must exist before you use this command. You can create the local user using user password first.

Format: `user <1-128> name name`

Mode: Captive Portal Configuration mode

**user group**

Use this command to associate a group with a captive portal user. A user must be associated with at least one group so the last group cannot be dis-associated. `<1-128>` is the user ID and `<1-10>` is the group ID.

Default: 1

Format: `user <1-128> group <1-10>`

Mode: Captive Portal Configuration mode

**no user group**

Use this command to dis-associate a group and user.

Format: `no user <1-128> group <1-10>`

Mode: Captive Portal Configuration mode

**user session-timeout**

Use this command to set the session timeout value for a captive portal user. Use the “no” form of this command to reset the session timeout to the default. The range of session timeout is 0-86400. 0 indicates use global configuration.

Default: 0

Format: `user <1-128> session-timeout timeout`

Mode: Captive Portal Configuration mode

**no user session-timeout**

Use this command to reset the session timeout to the default.

Format: `no user <1-128> session-timeout`

Mode: Captive Portal Configuration mode
**user idle-timeout**

Use this command to set the session idle timeout value for a captive portal user. `<1-128>` is the user ID. The range of idle timeout is 0-900 seconds. 0 indicates use global configuration.

Default

Format

Mode Captive Portal Configuration mode

**no user idle-timeout**

Use this command to reset the idle timeout to the default value.

Format

Mode Captive Portal Configuration mode

**user max-bandwidth-down**

Use this command to configure the bandwidth at which the client can receive data from the network. `<1-128>` is the user ID. The range of bps is `<0-536870911> bps`. 0 indicates use global configuration.

Default

Format

Mode Captive Portal Configuration mode

**no user max-bandwidth-down**

Use this command to reset the limit to the default.

Format

Mode Captive Portal Configuration mode

**user max-bandwidth-up**

Use this command to configure the bandwidth at which the client can send data into the Network. `<1-128>` is the user ID. The range of bps is `<0-536870911> bps`. 0 indicates use global configuration.

Default

Format

Mode Captive Portal Configuration mode
**no user max-bandwidth-up**

Use this command to reset the limit to the default.

**Format**

```
no user <1-128> max-bandwidth-up
```

**Mode**

Captive Portal Configuration mode

**user max-input-octets**

Use this command to limit the number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. `<1-128>` is the user ID. The range of `octets` is 0-4294967295. 0 indicates to use the global limit.

**Default**

0

**Format**

```
user <1-128> max-input-octets octets
```

**Mode**

Captive Portal Configuration mode

**no user max-input-octets**

Use this command to reset the limit to the default.

**Format**

```
no user <1-128> max-input-octets
```

**Mode**

Captive Portal Configuration mode

**user max-output-octets**

Use this command to limit the number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. The `<1-128>` is the user ID. The range of the `octets` is 0 – 4294967295. 0 indicates to use the global limit.

**Default**

0

**Format**

```
user <1-128> max-output-octets octets
```

**Mode**

Captive Portal Configuration mode

**no user max-output-octets**

Use this command to reset the limit to the default.

**Default**

0

**Format**

```
no user <1-128> max-output-octets
```

**Mode**

Captive Portal Configuration mode
**user max-total-octets**

Use this command to limit the number of bytes the user is allowed to transmit and receive. The maximum number of octets is the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. `<1-128>` is the user ID. The range of `octets` is 0-4294967295. 0 indicates to use the global limit. Use the “no” form of this command to reset the limit to the default.

Default 0
Format `user <1-128> max-total-octets octets`
Mode Captive Portal Configuration mode

**no user max-total-octets**

Use this command to reset the limit to the default.

Format `no user <1-128> max-total-octets`
Mode Captive Portal Configuration mode

**show captive-portal user**

Use this command to display all configured users or a specific user in the captive portal local user database.

Format `show captive-portal user [ <1-128> ]`
Mode Privileged EXEC mode

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user ID</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Logout once session timeout is reached (seconds). If the value is 0 then use</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Logout once idle timeout is reached (seconds). If the attribute is 0 then</td>
</tr>
<tr>
<td>Group ID</td>
<td>The group ID associated with the user</td>
</tr>
<tr>
<td>Group Name</td>
<td>The group name</td>
</tr>
</tbody>
</table>
If the user ID is specified, the following terms are displayed.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Configured</td>
<td>If the password is configured.</td>
</tr>
<tr>
<td>Max Bandwidth Up (bytes/sec)</td>
<td>Maximum client transmit rate (b/s). Limits the bandwidth at which the client can send data into the network. If the value is 0 then use the value configured for the captive portal.</td>
</tr>
<tr>
<td>Max Bandwidth Down (bytes/sec)</td>
<td>Maximum client receive rate (b/s). Limits the bandwidth at which the client can receive data from the network. If the value is 0 or then use the value configured for the captive portal.</td>
</tr>
<tr>
<td>Max Input Octets (bytes)</td>
<td>Maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. If the value is 0 then use the value configured for the captive portal.</td>
</tr>
<tr>
<td>Max Output Octets (bytes)</td>
<td>Maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. If the attribute is 0 then use the value configured for the captive portal.</td>
</tr>
<tr>
<td>Max Total Octets (bytes)</td>
<td>Maximum number of octets the user is allowed to transfer (sum of octets transmitted and received). After this limit has been reached the user will be disconnected. If the value is 0 then use the value configured for the captive portal.</td>
</tr>
</tbody>
</table>

**Example**

```
(switch)# show captive-portal user

User ID | User Name | Session | Idle
--------|-----------|---------|-------
1       | user123   | 10      | 13    |
2       | user234   | 0       | 0     |

(switch)# show captive-portal user 1

User ID................................. 1
User Name.............................. user123
Password Configured................... Yes
Session Timeout........................ 0
Idle Timeout........................... 0
Max Bandwidth Up (bytes/sec)......... 0
Max Bandwidth Down (bytes/sec)...... 0
Max Input Octets (bytes)............. 0
Max Output Octets (bytes)............ 0
Max Total Octets (bytes)............. 0
Group ID             | Group Name
-------- | ------------
1       | Default
2       | group2
```
**clear captive-portal users**

Use this command to delete all captive portal user entries.

**Format**
clear captive-portal users

**Mode**
Privileged EXEC mode

### Captive Portal User Group Commands

The following section describes captive portal user group commands.

**user group (Create)**

Use this command to create a user group. User group 1 is created by default and cannot be deleted.

**Default**
1

**Format**
user group <1-10>

**Mode**
Captive Portal Configuration mode

**no user group**

Use this command to delete a user group. The default user group (1) cannot be deleted.

**Format**
user group <1-10>

**Mode**
Captive Portal Configuration mode

**user group name**

Use this command to configure a group name. <1-10> is the user group ID. The name can be a string up to 32 characters.

**Format**
user group <1-10> name name

**Mode**
Captive Portal Configuration mode

**user group rename**

Use this command to change a group’s ID to a different group ID.

**Format**
user group group-id rename new-group-id

**Mode**
Captive Portal Configuration mode
Command List

{deny | permit} (IP ACL) ................................................................. 477
{deny | permit} (IPv6) ................................................................. 482
{deny | permit} (MAC ACL) .......................................................... 471
1583compatibility ................................................................. 270
aaa authentication dot1x ......................................................... 626
aaa authentication enable ....................................................... 625
aaa authentication login ......................................................... 624
aaa ias-user username ............................................................ 627
Absolute .......................................................... 486
access-list ............................................................ 475
cld-trapflags ............................................................ 479
addport ............................................................ 118
area default-cost (OSPF) ....................................................... 270
area default-cost (OSPFv3) ................................................... 380
area nssa (OSPF) ................................................................. 270
area nssa (OSPFv3) ............................................................... 380
area nssa default-info-originate (OSPF) ................................... 271
area nssa default-info-originate (OSPFv3) ................................ 381
area nssa no-redistribute (OSPF) ........................................... 271
area nssa no-redistribute (OSPFv3) ........................................ 381
area nssa no-summary (OSPF) ................................................. 272
area nssa no-summary (OSPFv3) .............................................. 382
area nssa translator-role (OSPF) .............................................. 272
area nssa translator-role (OSPFv3) ......................................... 382
area nssa translator-stab-intv (OSPF) ....................................... 272
area nssa translator-stab-intv (OSPFv3) ................................... 382
area range (OSPF) .............................................................. 273
area range (OSPFv3) ............................................................ 383
area stub (OSPF) ............................................................... 273
area stub (OSPFv3) .............................................................. 383
area stub no-summary (OSPF) ................................................. 274
area stub no-summary (OSPFv3) .............................................. 384
area virtual-link (OSPF) ....................................................... 274
area virtual-link (OSPFv3) ..................................................... 384
area virtual-link authentication .............................................. 274
area virtual-link dead-interval (OSPF) ..................................... 275
area virtual-link dead-interval (OSPFv3) ................................ 384
area virtual-link hello-interval (OSPF) ..................................... 275
area virtual-link hello-interval (OSPFv3) ................................ 385
area virtual-link retransmit-interval (OSPF) ............................................................... 276
area virtual-link retransmit-interval (OSPFv3) .............................................................. 385
area virtual-link transmit-delay (OSPF) ........................................................................... 276
area virtual-link transmit-delay (OSPFv3) ....................................................................... 386
arp ................................................................................................................................. 232
arp access-list ............................................................................................................... 157
arp cachesize .................................................................................................................. 233
arp dynamicrenew ......................................................................................................... 233
arp purge ......................................................................................................................... 233
arp resptime .................................................................................................................. 233
arp retries ......................................................................................................................... 234
arp timeout ..................................................................................................................... 234
assign-queue .................................................................................................................. 458
authentication timeout ................................................................................................... 692
authorization network radius .......................................................................................... 639
auto-cost (OSPF) ............................................................................................................ 277
auto-cost (OSPFv3) ......................................................................................................... 386
auto-negotiate ................................................................................................................ 39
auto-negotiate all ............................................................................................................ 39
auto-summary .................................................................................................................. 309
auto-voip ........................................................................................................................ 488
auto-voip all ................................................................................................................... 488
bandwidth ....................................................................................................................... 277
block ............................................................................................................................... 700
boot auto-copy-sw ......................................................................................................... 34
boot auto-copy-sw allow-downgrade ................................................................................ 35
boot auto-copy-sw trap ................................................................................................... 35
boot autoinstall start ...................................................................................................... 503
boot autoinstall stop ....................................................................................................... 503
boot host auto-save ........................................................................................................ 503
boot host dhcp ............................................................................................................... 504
boot host retry-count ..................................................................................................... 503
boot system .................................................................................................................... 505
bootfile ........................................................................................................................... 547
bootpdhcprelay cidoptmode .......................................................................................... 263
bootpdhcprelay maxhopcount ......................................................................................... 263
bootpdhcprelay minwaittime ......................................................................................... 264
bridge aging-time .......................................................................................................... 213
cablestatus ..................................................................................................................... 579
capability opaque ........................................................................................................... 278
captive-portal client deauthenticate ............................................................................... 708
captive-portal .................................................................................................................. 708
capture all packets ......................................................................................................... 560
capture receive packet .................................................................................................... 560
capture transmit packet ................................................................................................. 560
capture wrap ................................................................................................................... 561
class ............................................................................................................................... 459
class-map ......................................................................................................................... 449
class-map rename .......................................................................................................... 450
classofservice dot1p-mapping ......................................................................................... 441
classofservice ip-dscp-mapping ...................................................................................... 441
classofservice trust ........................................................................................................ 442
clear aaa ias-users .......................................................... 628
clear arp-cache ............................................................ 235
clear arp-switch ........................................................... 235
clear captive-portal users ................................................ 715
clear checkpoint statistics ............................................. 33
clear config ............................................................... 529
clear counters ............................................................. 529
clear dot1x authentication-history ................................... 98
clear dot1x statistics .................................................... 92
clear host ................................................................. 558
clear igmp-snooping ...................................................... 529
clear ip address-conflict-detect ..................................... 586
clear ip arp inspection statistics .................................... 159
clear ip dhcp binding ..................................................... 552
clear ip dhcp conflict ..................................................... 552
clear ip dhcp server statistics ........................................ 552
clear ip dhcp snooping binding ....................................... 152
clear ip dhcp snooping statistics .................................... 152
clear ip helper statistics ............................................... 265
clear ip ospf .............................................................. 278
clear ip ospf configuration ............................................ 278
clear ip ospf counters .................................................. 278
clear ip ospf neighbor .................................................. 279
clear ip ospf neighbor interface ..................................... 279
clear ip ospf redistribution ........................................... 279
clear ip ospf stub-router ............................................... 279
clear ip route all ......................................................... 244
clear ipv6 dhcp ........................................................... 414
clear ipv6 neighbors ...................................................... 368
clear ipv6 ospf ............................................................ 387
clear ipv6 ospf configuration ......................................... 387
clear ipv6 ospf counters ............................................... 387
clear ipv6 ospf neighbor ............................................... 387
clear ipv6 ospf neighbor interface .................................. 388
clear ipv6 ospf redistribution ........................................ 388
clear ipv6 statistics ..................................................... 375
clear isdp counters ....................................................... 217
clear isdp table ........................................................... 217
clear lldp remote-data .................................................. 189
clear lldp statistics ...................................................... 189
clear logging buffered ................................................ 529
clear logging email statistics ........................................ 525
clear mac-addr-table .................................................... 529
clear network ipv6 dhcp statistics .................................. 663
clear pass ................................................................. 530
clear port-channel ........................................................ 530
clear radius statistics ................................................... 92
clear traplog ............................................................... 530
clear vlan ................................................................. 530
client-identifier ......................................................... 544
client-name .............................................................. 544
clock summer-time date ............................................... 540
clock summer-time recurring ................................................................. 539
clock timezone .................................................................................. 539
configuration ..................................................................................... 539
configuration (Captive Portal) ............................................................... 594
conform-color ..................................................................................... 694
copy ....................................................................................................... 459
copy (pre-login banner) ........................................................................ 534
cos-queue min-bandwidth ..................................................................... 657
cos-queue min-bandwidth ..................................................................... 442
cos-queue random-detect ...................................................................... 443
cos-queue strict ................................................................................... 443
crypto certificate generate ...................................................................... 604
crypto key generate dsa ......................................................................... 604
crypto key generate rsa ......................................................................... 604
datacenter-bridging priority-flow-control mode on ............................... 221
datacenter-bridging priority-flow-control priority ................................. 221
debug arp ............................................................................................... 561
debug auto-voip ..................................................................................... 562
debug clear ............................................................................................ 562
debug console ....................................................................................... 562
debug dhcp packet ................................................................................ 562
debug dot1x packet ............................................................................... 563
debug igmpsnooping packet ................................................................... 564
debug igmpsnooping packet receive ...................................................... 565
debug igmpsnooping packet transmit .................................................... 564
debug ip acl .......................................................................................... 566
debug ip dvmrp packet .......................................................................... 566
debug ip igmp packet ............................................................................ 566
debug ip mcache packet ........................................................................ 567
debug ip pimdm packet ......................................................................... 567
debug ip pimsms packet ........................................................................ 568
debug ip vrrp ........................................................................................ 568
debug ipv6 dhcp ..................................................................................... 569
debug ipv6 mcache packet ..................................................................... 569
debug ipv6 mld packet .......................................................................... 570
debug ipv6 ospfv3 packet ...................................................................... 570
debug ipv6 pimdm packet ...................................................................... 574
debug ipv6 pimsms packet ..................................................................... 570
debug isdp packet ................................................................................ 571
debug lacp packet ................................................................................ 220
debug mldsnooping packet .................................................................... 571
debug ospf packet ............................................................................... 571
debug ping packet ................................................................................ 572
debug rip packet .................................................................................. 574
debug sflow packet .............................................................................. 575
debug spanning-tree bpdu ..................................................................... 576
debug spanning-tree bpdu receive ......................................................... 577
debug spanning-tree bpdu transmit ......................................................... 577
default-information originate (OSPF) .................................................... 279
default-information originate (OSPFv3) ................................................ 388
default-information originate (RIP) ....................................................... 310
default-metric (OSPF) .......................................................................... 280
default-metric (OSPFv3) ...................................................................... 388
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-metric (RIP)</td>
<td>310</td>
</tr>
<tr>
<td>default-router</td>
<td>545</td>
</tr>
<tr>
<td>delete</td>
<td>504</td>
</tr>
<tr>
<td>deleteport (Global Config)</td>
<td>119</td>
</tr>
<tr>
<td>deleteport (Interface Config)</td>
<td>119</td>
</tr>
<tr>
<td>description</td>
<td>40</td>
</tr>
<tr>
<td>dhcp client vendor-id-option</td>
<td>144</td>
</tr>
<tr>
<td>dhcp client vendor-id-option-string</td>
<td>144</td>
</tr>
<tr>
<td>dhcp l2relay</td>
<td>140</td>
</tr>
<tr>
<td>dhcp l2relay circuit-id vlan</td>
<td>140</td>
</tr>
<tr>
<td>dhcp l2relay remote-id vlan</td>
<td>141</td>
</tr>
<tr>
<td>dhcp l2relay trust</td>
<td>142</td>
</tr>
<tr>
<td>dhcp l2relay vlan</td>
<td>141</td>
</tr>
<tr>
<td>diffserv</td>
<td>449</td>
</tr>
<tr>
<td>disconnect</td>
<td>612</td>
</tr>
<tr>
<td>distance ospf (OSPF)</td>
<td>280</td>
</tr>
<tr>
<td>distance ospf (OSPFv3)</td>
<td>389</td>
</tr>
<tr>
<td>distance rip</td>
<td>310</td>
</tr>
<tr>
<td>distribute-list out (OSPF)</td>
<td>281</td>
</tr>
<tr>
<td>distribute-list out (RIP)</td>
<td>311</td>
</tr>
<tr>
<td>dns-server</td>
<td>545</td>
</tr>
<tr>
<td>dns-server (IPv6)</td>
<td>411</td>
</tr>
<tr>
<td>domain-name</td>
<td>547</td>
</tr>
<tr>
<td>domain-name (IPv6)</td>
<td>411</td>
</tr>
<tr>
<td>dos-control all</td>
<td>204</td>
</tr>
<tr>
<td>dos-control firstfrag</td>
<td>205</td>
</tr>
<tr>
<td>dos-control icmp</td>
<td>207</td>
</tr>
<tr>
<td>dos-control icmpfrag</td>
<td>212</td>
</tr>
<tr>
<td>dos-control icmpv4</td>
<td>211</td>
</tr>
<tr>
<td>dos-control icmpv6</td>
<td>211</td>
</tr>
<tr>
<td>dos-control l4port</td>
<td>206</td>
</tr>
<tr>
<td>dos-control sipdip</td>
<td>205</td>
</tr>
<tr>
<td>dos-control smacdmac</td>
<td>207</td>
</tr>
<tr>
<td>dos-control tcpfinurgrpsh</td>
<td>210</td>
</tr>
<tr>
<td>dos-control tcpflag</td>
<td>206</td>
</tr>
<tr>
<td>dos-control tcpflagseq</td>
<td>209</td>
</tr>
<tr>
<td>dos-control tcpfrag</td>
<td>206</td>
</tr>
<tr>
<td>dos-control tcpoffset</td>
<td>209</td>
</tr>
<tr>
<td>dos-control tcpport</td>
<td>208</td>
</tr>
<tr>
<td>dos-control tcpsyn</td>
<td>210</td>
</tr>
<tr>
<td>dos-control tcpsynfin</td>
<td>210</td>
</tr>
<tr>
<td>dos-control udpport</td>
<td>208</td>
</tr>
<tr>
<td>dot1x dynamic-vlan enable</td>
<td>98</td>
</tr>
<tr>
<td>dot1x guest-vlan</td>
<td>92</td>
</tr>
<tr>
<td>dot1x initialize</td>
<td>92</td>
</tr>
<tr>
<td>dot1x mac-auth-bypass</td>
<td>92</td>
</tr>
<tr>
<td>dot1x max-req</td>
<td>93</td>
</tr>
<tr>
<td>dot1x max-users</td>
<td>93</td>
</tr>
<tr>
<td>dot1x pae</td>
<td>105</td>
</tr>
<tr>
<td>dot1x port-control</td>
<td>94</td>
</tr>
<tr>
<td>dot1x port-control all</td>
<td>94</td>
</tr>
<tr>
<td>dot1x re-authenticate</td>
<td>95</td>
</tr>
</tbody>
</table>

**ProSafe Managed Switch**

---

**Command List**

720
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x re-authentication</td>
<td>95</td>
</tr>
<tr>
<td>dot1x supplicant max-start</td>
<td>106</td>
</tr>
<tr>
<td>dot1x supplicant port-control</td>
<td>105</td>
</tr>
<tr>
<td>dot1x supplicant timeout auth-period</td>
<td>107</td>
</tr>
<tr>
<td>dot1x supplicant timeout held-period</td>
<td>106</td>
</tr>
<tr>
<td>dot1x supplicant timeout start-period</td>
<td>106</td>
</tr>
<tr>
<td>dot1x supplicant user</td>
<td>107</td>
</tr>
<tr>
<td>dot1x system-auth-control</td>
<td>95</td>
</tr>
<tr>
<td>dot1x system-auth-control monitor</td>
<td>98</td>
</tr>
<tr>
<td>dot1x timeout</td>
<td>96</td>
</tr>
<tr>
<td>dot1x unauthenticated-vlan</td>
<td>97</td>
</tr>
<tr>
<td>dot1x user</td>
<td>97</td>
</tr>
<tr>
<td>drop</td>
<td>458</td>
</tr>
<tr>
<td>dvlan-tunnel ethertype</td>
<td>77</td>
</tr>
<tr>
<td>enable (OSPF)</td>
<td>269</td>
</tr>
<tr>
<td>enable (OSPFv3)</td>
<td>389</td>
</tr>
<tr>
<td>enable (Privileged EXEC access)</td>
<td>591</td>
</tr>
<tr>
<td>enable (RIP)</td>
<td>309</td>
</tr>
<tr>
<td>enable authentication</td>
<td>596</td>
</tr>
<tr>
<td>enable password</td>
<td>530</td>
</tr>
<tr>
<td>enable</td>
<td>691</td>
</tr>
<tr>
<td>enable (Instance)</td>
<td>694</td>
</tr>
<tr>
<td>encapsulation</td>
<td>243</td>
</tr>
<tr>
<td>exit-overflow-interval (OSPF)</td>
<td>281</td>
</tr>
<tr>
<td>exit-overflow-interval (OSPFv3)</td>
<td>390</td>
</tr>
<tr>
<td>external-lsdb-limit (OSPF)</td>
<td>281</td>
</tr>
<tr>
<td>external-lsdb-limit (OSPFv3)</td>
<td>390</td>
</tr>
<tr>
<td>ezconfig</td>
<td>589</td>
</tr>
<tr>
<td>filedescr</td>
<td>505</td>
</tr>
<tr>
<td>group</td>
<td>695</td>
</tr>
<tr>
<td>hardware-address</td>
<td>545</td>
</tr>
<tr>
<td>host</td>
<td>546</td>
</tr>
<tr>
<td>hostroutesaccept</td>
<td>312</td>
</tr>
<tr>
<td>http port</td>
<td>691</td>
</tr>
<tr>
<td>https port</td>
<td>691</td>
</tr>
<tr>
<td>idle-timeout</td>
<td>699</td>
</tr>
<tr>
<td>initiate failover</td>
<td>32</td>
</tr>
<tr>
<td>interface</td>
<td>38</td>
</tr>
<tr>
<td>interface lag</td>
<td>39</td>
</tr>
<tr>
<td>interface loopback</td>
<td>44</td>
</tr>
<tr>
<td>interface range</td>
<td>38</td>
</tr>
<tr>
<td>interface tunnel</td>
<td>354</td>
</tr>
<tr>
<td>interface vlan</td>
<td>38</td>
</tr>
<tr>
<td>interface (Captive Portal)</td>
<td>700</td>
</tr>
<tr>
<td>ip access-group</td>
<td>478</td>
</tr>
<tr>
<td>ip access-list</td>
<td>476</td>
</tr>
<tr>
<td>ip access-list rename</td>
<td>477</td>
</tr>
<tr>
<td>ip address</td>
<td>238</td>
</tr>
<tr>
<td>ip address dhcp</td>
<td>238</td>
</tr>
<tr>
<td>ip address-conflict-detect-run</td>
<td>585</td>
</tr>
<tr>
<td>ip arp inspection filter</td>
<td>156</td>
</tr>
<tr>
<td>ip arp inspection limit</td>
<td>156</td>
</tr>
</tbody>
</table>
Command List
ipv6 ospf area ................................................................. 376
ipv6 ospf cost ............................................................. 377
ipv6 ospf dead-interval ..................................................... 377
ipv6 ospf hello-interval .................................................... 377
ipv6 ospf mtu-ignore ....................................................... 378
ipv6 ospf network ......................................................... 378
ipv6 ospf priority .......................................................... 379
ipv6 ospf retransmit-interval ............................................ 379
ipv6 ospf transmit-delay .................................................. 380
ipv6 pim (Interface Config) .............................................. 420
ipv6 pim bsr-border ....................................................... 423
ipv6 pim bsr-candidate .................................................... 423
ipv6 pim dense(Global Config) .......................................... 420
ipv6 pim dr-priority ....................................................... 424
ipv6 pim hello-interval ................................................... 421
ipv6 pim join-prune-interval ............................................ 425
ipv6 pim register-rate-limit ............................................. 425
ipv6 pim rp-address ....................................................... 425
ipv6 pim rp-candidate ..................................................... 426
ipv6 pim spt-threshold ................................................... 426
ipv6 pim ssm ............................................................... 427
ipv6 route ................................................................. 358
ipv6 route distance ........................................................ 359
ipv6 router ospf .......................................................... 380
ipv6 traffic-filter ......................................................... 483
ipv6 unicast-routing ....................................................... 356
ipv6 unreachables .......................................................... 364
isdp advertise-v2 ........................................................... 216
isdp enable ................................................................. 216
isdp holdtime ............................................................. 215
isdp run ..................................................................... 215
isdp timer ................................................................. 216
key ......................................................................... 653
lacp actor admin .......................................................... 120
lacp actor admin key ....................................................... 120
lacp actor admin state individual ..................................... 120
lacp actor admin state longtimeout ................................... 121
lacp actor admin state passive ......................................... 121
lacp actor port priority ................................................... 122
lacp actor system priority ................................................. 122
lacp admin key ............................................................ 119
lacp collector max-delay ................................................ 119
lacp partner admin key ................................................... 123
lacp partner admin state individual .................................. 123
lacp partner admin state longtimeout ................................ 124
lacp partner admin state passive ...................................... 124
lacp partner port id ......................................................... 125
lacp partner port priority ................................................ 125
lacp partner system id ..................................................... 126
lacp partner system priority ............................................. 126
lease ....................................................................... 546
line ...................................................................... 594
match dstip6 ................................................................. 453
match dstl4port .......................................................... 453
match ethertype .......................................................... 451
match ip dscp ............................................................. 454
match ip precedence ..................................................... 454
match ip tos ............................................................... 454
match ip6flowlbl ........................................................ 452
match protocol ............................................................ 455
match secondary cos ..................................................... 452
match secondary-vlan ................................................... 457
match source-address mac .............................................. 456
match srcrip ............................................................... 456
match srcip6 .............................................................. 456
match srcl4port .......................................................... 456
match vlan ................................................................. 457
max-bandwidth-down ..................................................... 696
max-bandwidth-up ......................................................... 697
maximum-paths (OSPF) .................................................... 286
maximum-paths (OSPFv3) ................................................ 391
max-input-octets .......................................................... 697
max-output-octets ........................................................ 698
max-total-octets .......................................................... 698
member ....................................................................... 21
mirror .......................................................................... 458
mode dot1q-tunnel .......................................................... 77
mode dvlanc-tunnel ........................................................ 77
monitor session .............................................................. 134
movemanagement ........................................................... 23
mtu ............................................................................. 40
mvr ............................................................................ 223
mvr group ...................................................................... 224
mvr immediate ............................................................... 225
mvr mode ...................................................................... 224
mvr querytime ............................................................... 225
mvr type .................................................................. 226
mvr vlan ......................................................................... 225
mvr vlan group ............................................................. 226
name ........................................................................... 694
netbios-name-server ....................................................... 548
netbios-node-type .......................................................... 548
network (DHCP Pool Config) ............................................. 547
network area (OSPF) ......................................................... 269
network ipv6 address ....................................................... 660
network ipv6 enable ......................................................... 660
network ipv6 gateway ...................................................... 661
network javamode ........................................................... 592
network mac-address ....................................................... 591
network mac-type ............................................................ 592
network mgmt_vlan ........................................................ 64
network parms ................................................................. 591
network protocol ............................................................. 591
next-server ................................................................. 549
no [ietf] nsf restart-interval (OSPFv3) ................................................................. 409
no boot auto-copy-sw ............................................................. 35
no boot auto-copy-sw allow-downgrade ...................................... 35
no boot auto-copy-sw trap ............................................................ 35
no clock summer-time .................................................................. 541
no cos-queue random-detect ........................................................ 444
no ip vrrp vrid accept-mode ....................................................... 260
no lpf ......................................................................................... 587
no monitor .............................................................................. 135
no nsf ....................................................................................... 306
no nsf [ietf] (OSPFv3) ................................................................. 407
no nsf [ietf] helper strict-lsa-checking ...................................... 308
no nsf [ietf] helper strict-lsa-checking (OSPFv3) ...................... 409
no nsf helper ............................................................................ 307
no nsf helper (OSPFv3) ................................................................. 408
no nsf restart-interval ............................................................. 307
no random-detect exponential weighting-constant ..................... 444
no sdm prefer ........................................................................... 658
no set mld querier ................................................................. 180
no set mld querier election participate .................................... 181
no set mld querier query_interval ............................................. 180
no set mld querier timer expiry ................................................ 180
nsf ......................................................................................... 30
nsf (OSPFv3) ........................................................................... 407
nsf helper (OSPFv3) ................................................................. 407
nsf helper strict-lsa-checking (OSPFv3) .................................. 408
nsf ietf helper disable (OSPFv3) ............................................... 408
nsf restart-interval (OSPFv3) ...................................................... 409
option ..................................................................................... 549
passive-interface (OSPF) .......................................................... 287
passive-interface (OSPFv3) ......................................................... 391
passive-interface default (OSPF) ............................................... 287
passive-interface default (OSPFv3) .......................................... 391
password (AAA IAS User Configuration) .................................... 627
Password ................................................................................ 526
passwords aging ...................................................................... 618
passwords history .................................................................... 618
passwords lock-out .................................................................. 619
passwords min-length ............................................................... 617
passwords strength exclude-keyword ........................................ 622
passwords strength maximum consecutive-characters .............. 621
passwords strength maximum repeated-characters .................... 621
passwords strength minimum character-classes ....................... 622
passwords strength minimum lowercase-letters ......................... 620
passwords strength minimum numeric-characters ..................... 620
passwords strength minimum special-characters ....................... 621
passwords strength minimum uppercase-letters ......................... 621
passwords strength-check ............................................................. 487
periodic {start|end} time .............................................................. 486
periodic ................................................................................... 486
permit ip host mac host ........................................................... 157
ping ......................................................................................... 531
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping ipv6</td>
<td>532</td>
</tr>
<tr>
<td>ping ipv6 interface</td>
<td>533</td>
</tr>
<tr>
<td>poe</td>
<td>491</td>
</tr>
<tr>
<td>poe detection</td>
<td>491</td>
</tr>
<tr>
<td>poe high-power</td>
<td>492</td>
</tr>
<tr>
<td>poe power limit</td>
<td>492</td>
</tr>
<tr>
<td>poe power management</td>
<td>493</td>
</tr>
<tr>
<td>poe priority</td>
<td>494</td>
</tr>
<tr>
<td>poe reset</td>
<td>494</td>
</tr>
<tr>
<td>poe reset auto</td>
<td>495</td>
</tr>
<tr>
<td>poe timer schedule name</td>
<td>495</td>
</tr>
<tr>
<td>poe traps</td>
<td>496</td>
</tr>
<tr>
<td>poe usagethreshold</td>
<td>496</td>
</tr>
<tr>
<td>police-simple</td>
<td>461</td>
</tr>
<tr>
<td>police-two-rate</td>
<td>462</td>
</tr>
<tr>
<td>policy-map</td>
<td>462</td>
</tr>
<tr>
<td>policy-map rename</td>
<td>463</td>
</tr>
<tr>
<td>port</td>
<td>654</td>
</tr>
<tr>
<td>port lacpmode</td>
<td>127</td>
</tr>
<tr>
<td>port lacpmode enable all</td>
<td>127</td>
</tr>
<tr>
<td>port lacptimeout (Global Config)</td>
<td>128</td>
</tr>
<tr>
<td>port lacptimeout (Interface Config)</td>
<td>128</td>
</tr>
<tr>
<td>Port</td>
<td>526</td>
</tr>
<tr>
<td>port-channel adminmode</td>
<td>129</td>
</tr>
<tr>
<td>port-channel linktrap</td>
<td>129</td>
</tr>
<tr>
<td>port-channel load-balance</td>
<td>129</td>
</tr>
<tr>
<td>port-channel name</td>
<td>131</td>
</tr>
<tr>
<td>port-channel static</td>
<td>127</td>
</tr>
<tr>
<td>port-channel system priority</td>
<td>131</td>
</tr>
<tr>
<td>port-security</td>
<td>183</td>
</tr>
<tr>
<td>port-security mac-address</td>
<td>184</td>
</tr>
<tr>
<td>port-security mac-address move</td>
<td>184</td>
</tr>
<tr>
<td>port-security max-dynamic</td>
<td>183</td>
</tr>
<tr>
<td>port-security max-static</td>
<td>183</td>
</tr>
<tr>
<td>prefix-delegation (IPv6)</td>
<td>412</td>
</tr>
<tr>
<td>priority</td>
<td>654</td>
</tr>
<tr>
<td>private-group name</td>
<td>84</td>
</tr>
<tr>
<td>protocol group</td>
<td>70</td>
</tr>
<tr>
<td>protocol vlan group</td>
<td>71</td>
</tr>
<tr>
<td>protocol vlan group all</td>
<td>71</td>
</tr>
<tr>
<td>protocol</td>
<td>695</td>
</tr>
<tr>
<td>quit</td>
<td>533</td>
</tr>
<tr>
<td>radius accounting mode</td>
<td>639</td>
</tr>
<tr>
<td>radius server attribute</td>
<td>639</td>
</tr>
<tr>
<td>radius server host</td>
<td>640</td>
</tr>
<tr>
<td>radius server key</td>
<td>642</td>
</tr>
<tr>
<td>radius server msgauth</td>
<td>643</td>
</tr>
<tr>
<td>radius server primary</td>
<td>643</td>
</tr>
<tr>
<td>radius server retransmit</td>
<td>644</td>
</tr>
<tr>
<td>radius server timeout</td>
<td>644</td>
</tr>
<tr>
<td>random-detect exponential weighting-constant</td>
<td>444</td>
</tr>
<tr>
<td>random-detect queue-parms</td>
<td>444</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>redirect</td>
<td>459</td>
</tr>
<tr>
<td>redirect (Captive Portal)</td>
<td>696</td>
</tr>
<tr>
<td>redirect-url</td>
<td>696</td>
</tr>
<tr>
<td>redistribute (OSPF)</td>
<td>286</td>
</tr>
<tr>
<td>redistribute (OSPFv3)</td>
<td>392</td>
</tr>
<tr>
<td>redistribute (RIP)</td>
<td>313</td>
</tr>
<tr>
<td>release dhcp</td>
<td>239</td>
</tr>
<tr>
<td>reload</td>
<td>533</td>
</tr>
<tr>
<td>reload (Stack)</td>
<td>25</td>
</tr>
<tr>
<td>renew dhcp</td>
<td>239</td>
</tr>
<tr>
<td>router ospf</td>
<td>268</td>
</tr>
<tr>
<td>router rip</td>
<td>308</td>
</tr>
<tr>
<td>router-id (OSPF)</td>
<td>286</td>
</tr>
<tr>
<td>router-id (OSPFv3)</td>
<td>392</td>
</tr>
<tr>
<td>routing</td>
<td>237</td>
</tr>
<tr>
<td>save</td>
<td>533</td>
</tr>
<tr>
<td>script apply</td>
<td>656</td>
</tr>
<tr>
<td>script delete</td>
<td>656</td>
</tr>
<tr>
<td>script list</td>
<td>656</td>
</tr>
<tr>
<td>script show</td>
<td>656</td>
</tr>
<tr>
<td>script validate</td>
<td>657</td>
</tr>
<tr>
<td>sdm prefer</td>
<td>658</td>
</tr>
<tr>
<td>Security</td>
<td>525</td>
</tr>
<tr>
<td>serial baudrate</td>
<td>594</td>
</tr>
<tr>
<td>serial timeout</td>
<td>595</td>
</tr>
<tr>
<td>service dhcp</td>
<td>551</td>
</tr>
<tr>
<td>service dhcpv6</td>
<td>409</td>
</tr>
<tr>
<td>service-policy</td>
<td>463</td>
</tr>
<tr>
<td>session-limit</td>
<td>598</td>
</tr>
<tr>
<td>session-timeout</td>
<td>599</td>
</tr>
<tr>
<td>session-timeout (Captive Portal)</td>
<td>698</td>
</tr>
<tr>
<td>set garp timer join</td>
<td>85</td>
</tr>
<tr>
<td>set garp timer leave</td>
<td>86</td>
</tr>
<tr>
<td>set garp timer leaveall</td>
<td>86</td>
</tr>
<tr>
<td>set gmrp adminmode</td>
<td>89</td>
</tr>
<tr>
<td>set gmrp interfacemode</td>
<td>90</td>
</tr>
<tr>
<td>set gvrp adminmode</td>
<td>88</td>
</tr>
<tr>
<td>set gvrp interfacemode</td>
<td>88</td>
</tr>
<tr>
<td>set igmp</td>
<td>161</td>
</tr>
<tr>
<td>set igmp fast-leave</td>
<td>162</td>
</tr>
<tr>
<td>set igmp groupmembershipinterval</td>
<td>163</td>
</tr>
<tr>
<td>set igmp interfacemode</td>
<td>162</td>
</tr>
<tr>
<td>set igmp maxresponse</td>
<td>163</td>
</tr>
<tr>
<td>set igmp mctrxexpiretime</td>
<td>164</td>
</tr>
<tr>
<td>set igmp mrouter</td>
<td>165</td>
</tr>
<tr>
<td>set igmp mrouter interface</td>
<td>165</td>
</tr>
<tr>
<td>set igmp querier</td>
<td>169</td>
</tr>
<tr>
<td>set igmp querier election participate</td>
<td>171</td>
</tr>
<tr>
<td>set igmp querier query-interval</td>
<td>170</td>
</tr>
<tr>
<td>set igmp querier timer expiry</td>
<td>170</td>
</tr>
<tr>
<td>set igmp querier version</td>
<td>170</td>
</tr>
<tr>
<td>set igmp router-alert-check</td>
<td>165</td>
</tr>
</tbody>
</table>
set igmp unknow-multicast filter .................................................. 166
set mid ................................................................. 173
set mid fast-leave ............................................................ 174
set mid groupmembership-interval ........................................ 174
set mid interfacemode ......................................................... 173
set mid maxresponse ........................................................ 175
set mid mrouter .............................................................. 176
set mid mrouter interface ..................................................... 176
set prompt ................................................................. 657
set slot disable ............................................................. 24
set slot power ............................................................... 25
sflow poller ................................................................. 581
sflow receiver ............................................................... 580
sflow sampler ............................................................... 580
show aaa ias-users ........................................................ 628
show access-lists ............................................................ 481
show arp ................................................................. 235
show arp access-list ......................................................... 160
show arp brief ............................................................. 236
show arp switch ........................................................... 237
show arp switch ........................................................... 506
show authentication methods ............................................... 99
show auto-copy-sw ........................................................ 35
show autoinstall ........................................................... 502
show auto-voip ............................................................. 489
show bootpdhcprelay ......................................................... 264
show bootvar ............................................................... 505
show captive-portal client statistics ..................................... 706
show captive-portal client status ......................................... 704
show captive-portal configuration client status ..................... 707
show captive-portal configuration interface ......................... 701
show captive-portal configuration locales .......................... 704
show captive-portal configuration status ............................ 702
show captive-portal configuration ....................................... 700
show captive-portal interface client status ......................... 706
show captive-portal interface configuration status ................ 708
show captive-portal status ................................................. 693
show captive-portal trapflags ............................................ 704
show captive-portal user .................................................. 713
show captive-portal ....................................................... 692
show capture packets ....................................................... 561
show checkpoint statistics ................................................ 33
show class-map ............................................................ 465
show classofservice dot1p-mapping .................................... 445
show classofservice ip-dscp-mapping .................................. 446
show classofservice ip-precedence-mapping ......................... 446
show classofservice trust ................................................ 446
show clock ................................................................. 543
show datacenter-bridging priority-flow-control ..................... 222
show dhcp client vendor-id-option ...................................... 145
show dhcp l2relay agent-option vlan ................................. 143
Command List

ProSafe Managed Switch
ProSafe Managed Switch

show ip stats ............................................................ 250
show ip verify source .................................................... 153
show ip vlan .............................................................. 254
show ip vrrp .............................................................. 261
show ip vrrp interface ................................................... 261
show ip vrrp interface brief ............................................ 262
show ip vrrp interface stats ........................................... 260
show ipv6 access-lists ................................................ 484
show ipv6 brief ......................................................... 365
show ipv6 dhcp .......................................................... 412
show ipv6 dhcp binding ................................................ 415
show ipv6 dhcp interface ............................................... 414
show ipv6 dhcp pool .................................................... 415
show ipv6 dhcp statistics .............................................. 412
show ipv6 interface ..................................................... 366
show ipv6 mld groups .................................................. 431
show ipv6 mld interface ............................................... 432
show ipv6 mld traffic ................................................... 434
show ipv6 mld-proxy .................................................... 436
show ipv6 mld-proxy groups .......................................... 437
show ipv6 mld-proxy groups detail ................................ 438
show ipv6 mld-proxy interface ....................................... 437
show ipv6 mroute ....................................................... 418
show ipv6 mroute group ............................................... 419
show ipv6 mroute source ............................................. 419
show ipv6 neighbor .................................................... 368
show ipv6 ospf .......................................................... 394
show ipv6 ospf abr ..................................................... 397
show ipv6 ospf area .................................................... 397
show ipv6 ospf asbr .................................................... 398
show ipv6 ospf database .............................................. 399
show ipv6 ospf database database-summary ....................... 400
show ipv6 ospf interface .............................................. 400
show ipv6 ospf interface brief ...................................... 401
show ipv6 ospf interface stats ..................................... 402
show ipv6 ospf neighbor .............................................. 403
show ipv6 ospf range .................................................. 405
show ipv6 ospf stub table ............................................. 405
show ipv6 ospf virtual-link ......................................... 406
show ipv6 ospf virtual-link brief ................................... 406
show ipv6 pim .......................................................... 421
show ipv6 pim bsr-router ............................................ 427
show ipv6 pim interface .............................................. 422
show ipv6 pim neighbor ............................................... 422
show ipv6 pim rp mapping ............................................ 428
show ipv6 pim rp-hash ................................................ 428
show ipv6 route ........................................................ 368
show ipv6 route preferences ........................................ 370
show ipv6 route summary ............................................ 370
show ipv6 traffic ....................................................... 372
show ipv6 vlan ........................................................ 371
show isdp ............................................................... 217
show isdp entry ................................................................. 218
show isdp interface ............................................................ 218
show isdp neighbors ........................................................... 218
show isdp traffic ............................................................... 219
show lacp actor ............................................................... 131
show lacp partner ............................................................. 132
show license ...................................................................... 584
show license features .......................................................... 585
show lldp ........................................................................... 189
show lldp interface ............................................................. 189
show lldp local-device .......................................................... 193
show lldp local-device detail ................................................ 193
show lldp med ................................................................. 197
show lldp med interface ....................................................... 198
show lldp med local-device detail ........................................ 199
show lldp med remote-device ............................................... 201
show lldp med remote-device detail ..................................... 201
show lldp remote-device ...................................................... 191
show lldp remote-device detail ............................................. 192
show lldp statistics ............................................................ 190
show lpf interface all ........................................................ 587
show logging ................................................................. 518
show logging buffered ....................................................... 519
show logging email config ................................................ 524
show logging email statistics ............................................... 524
show logging hosts .......................................................... 519
show logging traplogs ........................................................ 520
show loginsession ............................................................ 612
show mac access-lists ......................................................... 473
show mac-address-table gmrp ............................................. 91
show mac-address-table igmp-snooping ................................ 168
show mac-address-table mldsnooping .................................. 178
show mac-address-table multicast ...................................... 214
show mac-address-table static .......................................... 139
show mac-address-table staticfiltering ................................ 139
show mac-address-table stats ............................................ 215
show mac-addr-table ........................................................ 510
show mail-server config .................................................... 526
show mbuf total ............................................................... 512
show mldsnooping ........................................................... 177
show mldsnooping mrouter interface ................................... 178
show mldsnooping mrouter vlan ......................................... 178
show monitor session ......................................................... 135
show mvr ................................................................. 227
show mvr interface ........................................................... 228
show mvr members .......................................................... 227
show mvr traffic .............................................................. 229
show network ................................................................. 592
show network ipv6 dhcp statistics ........................................ 662
show network ndp ............................................................ 661
show nsf ................................................................ 31
show passwords configuration ............................................ 623
show passwords result 623
show poe 497
show poe pd 500
show poe port configuration 498
show poe port info 499
show policy-map 466
show policy-map interface 469
show port 42
show port description 43
show port protocol 43
show port status 44
show port-channel 133
show port-channel brief 132
show port-channel system priority 134
show port-security 184
show port-security dynamic 185
show port-security static 185
show port-security violation 185
show private-group 85
show process cpu 512
show radius 645
show radius accounting 647
show radius accounting statistics 648
show radius servers 646
show radius statistics 650
show running-config 514
show running-config interface 513
show sdm prefer 658
show serial 596
show service-policy 469
show sflow agent 582
show sflow pollers 582
show sflow receivers 583
show sflow samplers 583
show slot 25
show snmpcommunity 636
show snmptrap 637
show sntp 541
show sntp client 541
show snntp server 542
show spanning-tree 56
show spanning-tree brief 57
show spanning-tree interface 58
show spanning-tree mst port detailed 58
show spanning-tree mst port summary 61
show spanning-tree mst port summary active 61
show spanning-tree mst summary 62
show spanning-tree summary 62
show spanning-tree vlan 63
show stack-port 29
show stack-port counters 29
show stack-port diag .............................................................. 30
show storm-control ............................................................. 117
show supported cardtype ..................................................... 26
show supported switchtype ................................................... 28
show switch ................................................................. 27
show switchport protected .................................................. 83
show sysinfo ............................................................... 514
show tacacs ................................................................. 654
show tech-support ............................................................ 514
show telnet ................................................................. 600
show telnetcon ............................................................... 601
show terminal length ......................................................... 515
show time-range ............................................................ 487
show trapflags ............................................................... 638
show users ................................................................. 615
show users accounts ........................................................ 616
show users login-history .................................................... 617
show users long ............................................................. 617
show version ............................................................... 507
show vlan ................................................................. 73
show vlan <vlanid> .......................................................... 74
show vlan association mac .................................................. 76
show vlan association subnet ............................................... 76
show vlan brief ........................................................... 75
show vlan port .............................................................. 75
show voice vlan ............................................................. 80
shutdown ................................................................. 40
shutdown all ............................................................... 41
slot ........................................................................... 23
snmp trap link-status ....................................................... 635
snmp trap link-status all .................................................... 636
snmp-server ............................................................... 628
snmp-server community .................................................... 628
snmp-server community ipaddr ........................................... 629
snmp-server community ipmask .......................................... 629
snmp-server community mode .......................................... 630
snmp-server community ro ............................................... 631
snmp-server community rw ............................................... 631
snmp-server enable traps .................................................. 631
snmp-server enable traps linkmode ..................................... 632
snmp-server enable traps multiusers ................................... 632
snmp-server enable traps stpmode ...................................... 633
snmp-server enable traps violation ..................................... 631
snmptrap ................................................................. 631
snmptrap ipaddr ........................................................... 633
snmptrap mode ............................................................ 634
snmptrap snmpversion ....................................................... 634
snntp broadcast client poll-interval ..................................... 536
snntp client mode ........................................................ 537
snntp client port .......................................................... 537
snntp server .............................................................. 539
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>sntp unicast client poll-interval</td>
<td>537</td>
</tr>
<tr>
<td>sntp unicast client poll-retry</td>
<td>538</td>
</tr>
<tr>
<td>sntp unicast client poll-timeout</td>
<td>538</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>46</td>
</tr>
<tr>
<td>spanning-tree bpdufilter</td>
<td>46</td>
</tr>
<tr>
<td>spanning-tree bpdufilter default</td>
<td>46</td>
</tr>
<tr>
<td>spanning-tree bpduflood</td>
<td>47</td>
</tr>
<tr>
<td>spanning-tree bpduforwarding</td>
<td>55</td>
</tr>
<tr>
<td>spanning-tree bpduguard</td>
<td>47</td>
</tr>
<tr>
<td>spanning-tree bpdumigrationcheck</td>
<td>48</td>
</tr>
<tr>
<td>spanning-tree configuration name</td>
<td>48</td>
</tr>
<tr>
<td>spanning-tree configuration revision</td>
<td>48</td>
</tr>
<tr>
<td>spanning-tree edgeport</td>
<td>49</td>
</tr>
<tr>
<td>spanning-tree edgeport all</td>
<td>55</td>
</tr>
<tr>
<td>spanning-tree forceversion</td>
<td>49</td>
</tr>
<tr>
<td>spanning-tree forward-time</td>
<td>50</td>
</tr>
<tr>
<td>spanning-tree guard</td>
<td>50</td>
</tr>
<tr>
<td>spanning-tree max-age</td>
<td>51</td>
</tr>
<tr>
<td>spanning-tree max-hops</td>
<td>51</td>
</tr>
<tr>
<td>spanning-tree mst</td>
<td>52</td>
</tr>
<tr>
<td>spanning-tree mst instance</td>
<td>53</td>
</tr>
<tr>
<td>spanning-tree mst priority</td>
<td>53</td>
</tr>
<tr>
<td>spanning-tree mst vlan</td>
<td>54</td>
</tr>
<tr>
<td>spanning-tree port mode</td>
<td>54</td>
</tr>
<tr>
<td>spanning-tree port mode all</td>
<td>55</td>
</tr>
<tr>
<td>spanning-tree tcnguard</td>
<td>50</td>
</tr>
<tr>
<td>speed</td>
<td>41</td>
</tr>
<tr>
<td>speed all</td>
<td>42</td>
</tr>
<tr>
<td>split-horizon</td>
<td>313</td>
</tr>
<tr>
<td>sshcon maxsessions</td>
<td>602</td>
</tr>
<tr>
<td>sshcon timeout</td>
<td>603</td>
</tr>
<tr>
<td>stack</td>
<td>21</td>
</tr>
<tr>
<td>stack-port</td>
<td>29</td>
</tr>
<tr>
<td>standby</td>
<td>23</td>
</tr>
<tr>
<td>storm-control broadcast</td>
<td>108</td>
</tr>
<tr>
<td>storm-control broadcast (Global)</td>
<td>109</td>
</tr>
<tr>
<td>storm-control broadcast level</td>
<td>108</td>
</tr>
<tr>
<td>storm-control broadcast level (Global)</td>
<td>110</td>
</tr>
<tr>
<td>storm-control broadcast rate</td>
<td>109</td>
</tr>
<tr>
<td>storm-control broadcast rate (Global)</td>
<td>110</td>
</tr>
<tr>
<td>storm-control flowcontrol</td>
<td>116</td>
</tr>
<tr>
<td>storm-control multicast</td>
<td>111</td>
</tr>
<tr>
<td>storm-control multicast (Global)</td>
<td>112</td>
</tr>
<tr>
<td>storm-control multicast level</td>
<td>111</td>
</tr>
<tr>
<td>storm-control multicast level (Global)</td>
<td>112</td>
</tr>
<tr>
<td>storm-control multicast rate</td>
<td>112</td>
</tr>
<tr>
<td>storm-control multicast rate (Global)</td>
<td>113</td>
</tr>
<tr>
<td>storm-control unicast</td>
<td>113</td>
</tr>
<tr>
<td>storm-control unicast (Global)</td>
<td>115</td>
</tr>
<tr>
<td>storm-control unicast level</td>
<td>114</td>
</tr>
<tr>
<td>storm-control unicast level (Global)</td>
<td>115</td>
</tr>
<tr>
<td>storm-control unicast rate</td>
<td>114</td>
</tr>
</tbody>
</table>
Command List

storm-control unicast rate (Global) ................................................................. 116
switch priority .................................................................................................. 22
switch renumber ............................................................................................... 22
switchport private-group ................................................................................. 84
switchport protected (Global Config) ............................................................. 82
switchport protected (Interface Config) ......................................................... 82
tacacs-server host ......................................................................................... 652
tacacs-server key ............................................................................................ 652
tacacs-server timeout .................................................................................... 653
telnet ................................................................................................................ 597
telnetcon maxsessions .................................................................................... 599
telnetcon timeout .......................................................................................... 600
terminal length ............................................................................................... 615
timeout ............................................................................................................ 615
time-range ...................................................................................................... 485		
timers spf ........................................................................................................ 287
traceroute ........................................................................................................ 527
traceroute ipv6 ................................................................................................. 528
traffic-shape .................................................................................................... 445
transport input telnet ....................................................................................... 597
transport output telnet ..................................................................................... 598
trapflags (OSPF) ............................................................................................ 288
trapflags (OSPFv3) ........................................................................................ 393
tunnel destination ........................................................................................... 354
tunnel mode ipv6ip ......................................................................................... 355
tunnel source ................................................................................................. 354
update bootcode ............................................................................................. 505
user group (Create) ......................................................................................... 715
user group name ............................................................................................. 715
user group rename .......................................................................................... 715
user group ........................................................................................................ 710
user idle-timeout ............................................................................................. 711
user max-bandwidth-down ............................................................................. 711
user max-bandwidth-up ................................................................................... 711
user max-input-octets ..................................................................................... 712
user max-output-octets ................................................................................... 712
user max-total-octets ...................................................................................... 713
user name ........................................................................................................ 710
user password ................................................................................................. 709
user session-timeout ....................................................................................... 710
username ......................................................................................................... 613
username <username> unlock ....................................................................... 614
username nopassword ..................................................................................... 613
username snmpv3 accessmode ..................................................................... 614
username snmpv3 authentication .................................................................. 614
username snmpv3 encryption ....................................................................... 615
Username .......................................................................................................... 526
verification ...................................................................................................... 695
vlan .................................................................................................................. 64
vlan acceptframe ............................................................................................ 65
vlan association mac ....................................................................................... 73
vlan association subnet .................................................................................... 73
vlan database ................................................................. 64
vlan ingressfilter .......................................................... 65
vlan makestatic ............................................................. 66
vlan name ................................................................. 66
vlan participation ......................................................... 66
vlan participation all ..................................................... 67
vlan port acceptframe all ................................................ 67
vlan port ingressfilter all ............................................... 68
vlan port priority all ...................................................... 81
vlan port pvid all ........................................................ 68
vlan port tagging all ...................................................... 69
vlan priority .............................................................. 81
vlan protocol group ....................................................... 69
vlan protocol group add protocol ....................................... 70
vlan protocol group name ................................................ 69
vlan pvid ................................................................. 72
vlan routing .............................................................. 253
vlan tagging .............................................................. 72
voice vlan (Global Config) ............................................... 79
voice vlan (Interface Config) ............................................ 79
voice vlan data priority .................................................. 80
write memory ............................................................ 536